Cukurova University Journal of Natural & Applied Sciences (2024) 3(2): 45-52

e-ISSN: 2822-2938

Cukurova University Journal of Natural & Applied Sciences

Original Paper

Comparative Analysis of Face Recognition Algorithms for Facial Recognition in Diverse Environments

Üsame DURAK[1], Ayşegül Ceren KOÇ[1], Hüseyin DAŞ[1], Oğuzhan KARAHAN[1], M. Fatih KILIÇ[1], M. Fatih AKAY[2]

[1]Biges Güvenli Hayat Teknolojiler A.Ş., R&D Department, Istanbul, Turkey
[2]Cukurova University, Department of Computer Engineering, Adana, Turkey

ORCID IDs of the authors: Ü.D. 0000-0003-1723-3444; A.C.K. 0000-0001-5519-3231; H.D. 0000-0003-4254-413X; O.K. 0000-0002-8571-5528; M.F.K. 0000-0002-5596-7097; M.F.A. 0000-0003-0780-0679.

Cite this article as: Durak, Ü., Koç, A.C., Daş, H., Karahan, O., Kılıç M.F., Akay, M.F. (2024). Comparative Analysis of Face Recognition Algorithms for Facial Recognition in Diverse Environments, Cukurova University Journal of Natural & Applied Sciences 3(2): 45-52. https://doi.org/10.70395/cunas.1504238.

Abstract

Facial recognition technology has evolved significantly over the last five decades and plays a central role in various applications such as biometrics, information security, access control, law enforcement and surveillance. In this study, the performance of two face recognition algorithms, Dlib and FaceNet, is evaluated using datasets obtained from video recordings in different environments. The Dlib algorithm uses the Histogram of Oriented Gradients (HOG) method for face detection, while FaceNet uses the Multi-Task Cascaded Convolutional Neural Network (MTCNN). The experimental results show that both algorithms achieve high accuracy in controlled environments, with Dlib showing greater robustness in complex scenarios. This study makes an important contribution to this topic by presenting a comparative analysis of the face recognition performance of the OpenFace, ArcFace, Exadel, and Dlib methods under different environmental conditions and scenarios. The results show that while the tested methods achieve high accuracy in controlled environments, their performance differs in more complex environments. In the results, OpenFace and ArcFace showed lower success rates than the other two algorithms. In particular, Dlib proved superior in dynamic and challenging scenarios, achieving an overall accuracy of 96.1% compared to 94.6% for Exadel. Exadel, on the other hand, performed slightly better in certain controlled environments, highlighting its potential strength in certain applications. These results emphasize the importance of selecting the appropriate algorithm based on the specific environmental conditions and requirements of the application. This research not only improves our understanding of the performance characteristics of leading facial recognition technologies, but also provides practical insights into their use in real-world applications.

Keywords: Face recognition, FaceNet, Dlib, Exadel, CCTV, Alarm Systems

1. Introduction

In today's digital age, facial recognition technology has evolved into a powerful tool with wide-ranging applications in various fields. What began nearly five decades ago as a nascent field of research in pattern recognition and computer vision has now evolved into a sophisticated technology capable of identifying individuals with remarkable accuracy. This technological advancement has paved the way for widespread application in areas such as biometrics, information security, access control, law enforcement, smart cards, and surveillance systems.

Rapid advances in computer technology have catapulted facial recognition systems to new heights, surpassing human capabilities in many tasks. With the ability to analyze and match facial features with unprecedented precision, these systems have become indispensable when it comes to enhancing security, streamlining identification processes, and enabling efficient surveillance in various scenarios. The proliferation of facial recognition technology has sparked discussions about privacy, ethical considerations,

Address for Correspondence:
Üsame Durak, e-mail: usame.durak@hybrone.com

Received: Jun 26, 2024
Accepted: Aug 1, 2024

and the need for responsible implementation. Finding the right balance between the benefits of this technology and dealing with potential risks remains a key challenge for societies worldwide [1].

However, the proliferation of facial recognition technology has triggered discussions about privacy, ethical considerations and the need for responsible implementation. The collection and storage of biometric data raises significant concerns about data security and potential misuse. In addition, the use of facial recognition systems in public spaces has led to debates about individual privacy rights and the potential for mass surveillance. To gain public trust and achieve social acceptance, it is important to ensure that these technologies are used in an ethical and transparent manner.

Finding the right balance between the benefits of this technology and dealing with potential risks remains a key challenge for societies worldwide. Policymakers, technologists, and ethicists need to work together to develop robust frameworks for the use of facial recognition technology. These frameworks should address issues such as consent, privacy, algorithmic bias, and accountability. By promoting a multidisciplinary approach, it is possible to harness the potential of facial recognition technology while protecting individual rights and promoting ethical standards.

2. Literature Review

Ahmed A. Elngar and Mohammed Kayed propose a vehicle surveillance and alarm system that uses biometric authentication based on IoT technology to enhance vehicle security. The system, called VSS-IoT, uses a Raspberry Pi 3 Model B+ development board, a Pi camera, a PIR sensor, and a smartphone interface to grant full access only to authorized drivers. The proposed algorithm uses the Haar cascade method to detect faces and a customized PCA algorithm for identification. The VSS-IoT achieved an accuracy of 98.2% on the ORL dataset and 99.6% on their own dataset [2].

According to the study by Dhimas Tribuana et al. [3], a compact model was developed using MobileNet V2 and Transfer Learning for the Raspberry Pi platform, which contains five facial recognition classes and one class for unknown faces. The model showed an accuracy of 97.29%, a perfect recognition of 100% and a precision of 89.7%, making it an effective and feasible solution for secure access control in office environments [3].

In their study, Sergei Shavetov and Vladimir Sivtsov conducted a comparative analysis of face detection algorithms, including MTCNN, FD-CNN, and Viola Jones. In the test results with the FDDB dataset (5171 faces from 2845 images), MTCNN showed superior performance, achieving an Area Under the Curve (AUC) value of 0.944. In addition, FaceNet was used due to its superior performance in face recognition in the LFW dataset, using a deep learning-based approach to detect spoofing attempts. Moreover, to improve the performance of the proposed system, the system uses image processing techniques such as image resizing, face cropping, and sharpening [4].

In another work, a CNN framework developed for robust face recognition in uncontrolled environments is presented. This study emphasizes the effectiveness and flexibility of the model by using aggressive data augmentation and an adaptive fusion strategy. In particular, the high success rates of 99.2% on the LFW dataset and 96.63% on the YTF dataset emphasise the effectiveness of this approach. Their model approaches the accuracy rate of FaceNet by about 0.66%. Ultimately, FaceNet was trained on a large database of 200 million photos of eight million people [5].

In a survey by Li et al. [6], face recognition technology is explored from various perspectives, encompassing its development stages, underlying technologies, research on real-world applications, evaluation metrics, standard databases, and future directions. The authors perform a comparative analysis of various datasets, considering factors like the number of individuals included, image variations, and difficulty levels. Additionally, they compile successful methodologies employed within these datasets and offer a comprehensive survey of existing techniques present in the current literature [6].

In this study, the Dlib face recognition algorithm, available via the repository on GitHub, and the FaceNet algorithm, implemented via the open source project Exadel, were used. The OpenFace and ArcFace algorithms, available via the repository on GitHub DeepFace. The facial recognition performance of these four systems was tested on four self-generated datasets. The test samples, which originate from video recordings, were processed according to specific guidelines in order to obtain meaningful results. The results of these four approaches were compared and reported to evaluate their effectiveness in face recognition [7, 8, 9].

Table 1. Comparison of Studies in the Literature with Our Study

Algorithm/Technique	Accuracy (%)	Dataset	Authors
AlexNet	100	ORL	Atsu et al. [10]
LeNet	96.67	YALE	Atsu et al. [10]
SVM + PCA	88	Custom	Radhika et al. [11]
MLP + LDA	87	Custom	Radhika et al. [11]
CNN	98	Custom	Radhika et al. [11]
DCNN + DeepFace / ArcFace	87.5	Custom	Özlem Güven [12]
Dlib	96.1	Ours	-

Various literature studies were searched and the performance of the algorithms was compared, as shown in Table 1. In the study conducted by Atsu Alagah Komlavi and his team, the results of certain models were shared on two different datasets. The study concluded that deep learning-based models perform better with increasing data size. Among these studies, the best results were obtained by AlexNet on the ORL dataset and by LeNet on the YALE dataset. The ORL dataset contains 400 images from 40 different individuals, while the YALE dataset contains 165 images from 11 different individuals. AlexNet achieved an accuracy of 100% on the ORL dataset, while LeNet achieved an accuracy of 96.67% on the YALE dataset [10]. In the study conducted by Radhika C. Damale and his team, a custom dataset was used, but no information was provided on the size of the dataset. In this study, the highest accuracy rates were achieved by CNN, SVM+PCA and MLP+LDA with 98%, 88% and 87% accuracy, respectively [11]. Özlem Güven's study aimed to identify and authorize drivers. The data collected from her own drivers included 578 images of 50 different people. The tests conducted with DCNN + DeepFace / ArcFace achieved an accuracy of 87.5% [12]. The above comparisons clearly show the performance of the different studies on different datasets. Using this analysis, we compared and evaluated our own results with existing work in the literature.

The use of different video datasets created by the researchers allowed for an exemplary application study that significantly expanded the scope of the work by using a higher number of video samples compared to many existing studies in the literature. Careful consideration of the distribution of different individuals, genders, and age groups makes the study's contribution to the literature even greater. This approach enables a detailed evaluation of the performance of face recognition algorithms in different demographic groups. The comprehensive test conditions used in the study take into account possible biases that can occur in face recognition systems.

Compared to the existing literature, this study provides a unique contribution by specifically analyzing the performance of OpenFace, ArcFace, Dlib, and Exadel FaceNet in different real world environments. Previous studies often focus on controlled environments and provide limited insight into real world applicability. For example, previous research on Dlib has typically emphasized its effectiveness in static environments with uniform illumination and minimal occlusion without thoroughly investigating its robustness in dynamic scenarios. Similarly, studies on FaceNet have largely focused on its high accuracy in benchmark datasets, but without thoroughly investigating its performance under different environmental conditions.

Our study fills this gap by providing empirical evidence of how these algorithms perform in both controlled and complex, real-world environments. This comparative analysis underscores the need to evaluate face recognition algorithms beyond standard benchmarks, taking into account real world challenges.

3. Material and Method

This section describes the dataset used and the methods used for face detection, face embedding, and face identification. The dataset consists of video recordings from different locations showing people in different scenarios. Advanced algorithms are used to recognize faces in these videos. Subsequently, face embeddings are generated using architectures such as FaceNet and Dlib. The final step is face identification, where algorithms predict identities based on these embeddings. The experimental setup outlines the rules and procedures for processing the videos and evaluating the facial recognition systems.

3.1 Data Sets

The recordings include scenarios in which people move from about 5 meters away to 1-2 meters close to the camera. For the testing processes, 4 datasets were created with video records collected from different locations. The videos were recorded at the following locations: Biges Warehouse (16 videos), Hybrone Turnstile Area (61 videos), Biges Office Room(31 videos), and the Hybrone Test Room (22 videos). These different settings enable a comprehensive view of the test subjects from different perspectives.

These test videos record people from CCTV cameras positioned at a maximum distance of 5 meters. The people can enter the frame either at the beginning or at any point during the video. Although different cameras were used, all videos in this set were recorded at a high shutter speed of 25 fps and a resolution of 1920x1080.

3.2 Face Detection

Facial detection is the process of identifying and localizing human faces in images or videos. It is a crucial first step in many facial recognition and analysis systems. This process usually involves the use of machine learning models that are trained to recognize facial features and distinguish them from other objects in the image. Once a face has been recognized, the system can analyze and process the facial data for various applications such as authentication, tracking, and identification [13].

Dlib

Dlib uses the Histogram of Oriented Gradients (HOG) method for face detection, which captures the distribution of gradient orientations in an image to identify facial features. This method is known for its accuracy and efficiency in recognizing faces in images and videos [7, 14].

Exadel

Exadel uses the Multi-Task Cascaded Convolutional Neural Network (MTCNN) for face detection, a deep learning-based method known for its robustness in detecting faces under different conditions [11]. MTCNN uses a cascaded architecture to detect faces at different scales and accurately localize facial features [8, 15].

RetinaFace

RetinaFace is a cutting-edge facial detection algorithm using deep learning to achieve high accuracy and robustness. It employs a multi-task learning framework for face detection, landmark localization, and pose estimation. This algorithm has shown superior performance on benchmark datasets, making it widely adopted in research and practical applications [16].

3.3 Face Embedding

Face embedding is a technique used to represent facial images as numerical vectors in a high-dimensional space to capture the unique features of each face. Algorithms such as FaceNet and Dlib are commonly used to generate face embeddings and enable efficient comparison and recognition of faces [17].

FaceNet

FaceNet, a deep learning architecture developed by Google, achieves remarkable performance with an accuracy of 99.58% on the Labeled Faces in the Wild (LFW) dataset, proving its efficiency in facial recognition under different conditions and in different environments [18].

Dlib

The Dlib face embedding algorithm uses a metric learning approach based on deep metric learning techniques, enabling accurate verification of face pairs. This algorithm achieves high performance in determining whether two facial images belong to the same person or not, which makes it suitable for face recognition tasks [19].

OpenFace

OpenFace is a leading facial recognition algorithm that uses deep learning to provide high accuracy and flexibility. It is designed for facial landmark detection and face alignment, offering robust performance on various datasets. This algorithm is widely used in both research and practical applications due to its open-source availability and effectiveness [20].

ArcFace

ArcFace is an advanced facial recognition algorithm that leverages deep learning to deliver superior accuracy and robustness. It utilizes an additive angular margin loss to enhance discriminative feature learning, improving face verification and identification. ArcFace has consistently outperformed other methods on benchmark datasets, making it a preferred choice in academic and practical settings [21].

3.4 Face Verification

Face verification is the identity of a person that is determined on the basis of their facial image. The facial features extracted from an input image are compared with the features stored in a database of known faces so that the system can identify the person if a match is found. Both the Exadel and Dlib methods use the Euclidean distance metric to compare the feature vectors extracted from the facial images. Both the ArcFace and OpenFace methods use the Cosine distance metric to compare the feature vectors extracted from the facial images. This comparison allows the systems to measure the similarity between faces and determine whether they belong to the same person. This method is often used in security systems, access control, and personalized services [22, 23].

3.5 Experimental Setup

The experiments were conducted on a high-performance computer system to ensure accurate and efficient processing of the face recognition tasks. The hardware setup for conducting these experiments includes an NVIDIA 3090ti GPU, which provides significant computing power for processing complex algorithms and large data sets. The system is equipped with 24 CPU cores, 64 GB of RAM and a 2 TB SSD for ample storage capacity. This robust configuration enables the execution of intensive facial recognition processes.

A data set with 5 female and 2 male photos was integrated into the systems for OpenFace, ArcFace, Dlib, and Exadel methods. Subsequently, the images extracted from the videos using the Dlib-based method were subjected to prediction. After prediction, the individual with the highest number of predictions (at least 3 predictions with more than 0.6 confidence) was determined as the final prediction. In cases where there were less than 3 predictions, the result was classified as an unknown individual.
In the Exadel system, the face recognition results were compared with the confidence intervals (between 0.99 and 0.9) extracted from the video images. Rules were then established on the basis of these confidence intervals:

1. Predictions with a confidence interval above 0.98 and a single occurrence were considered correct.
2. For predictions with a confidence interval above 0.98 and 4 or more occurrences, the individual with the highest predictions was considered correct.
3. Predictions with a confidence interval above 0.95 and a single occurrence associated with 8 or more predictions were considered correct.
4. For predictions with a confidence interval greater than 0.95 and 20 or more occurrences, the individual with the highest predictions was considered correct.
5. For predictions with a confidence interval of over 0.90 and 25 or more occurrences, the individual with the most predictions was considered correct.

Both OpenFace and ArcFace methods use RetinaFace for face detection. For OpenFace, more than 5 guesses made by the same person in the video are considered as final prediction, while for ArcFace, this number is chosen as 10. This methodology was applied to all videos to evaluate the performance of both methods.

4. Results and Discussion

The results of our experiments, in which we evaluated the face recognition performance of the OpenFace, ArcFace, Exadel, and Dlib methods on different test sets, show remarkable differences in terms of accuracy, computational efficiency, and robustness to various challenging scenarios. All methods were tested on the same test datasets.

Table 2. Comparative Analysis of ArcFace, OpenFace, Dlib and FaceNet for Accuracy in Different Environments

Environment	Number of Videos	ArcFace	OpenFace	Exadel	Dlib
Biges Warehouse	16	100%	100%	100%	100%
Hybrone Turnstile Area	61	95.10%	62.20%	93.40%	98.30%
Hybrone Test Room	22	100%	22.70%	100%	100%
Biges Office Room	31	74.20%	25.80%	90.30%	87.10%
Overall	130	91.54%	51.48%	94.59%	96.12%

Table 3. Comparative Analysis of ArcFace, OpenFace, Dlib and FaceNet for Precision in Different Environments

Environment	ArcFace	OpenFace	Exadel	Dlib
Biges Warehouse	100%	100%	100%	100%
Hybrone Turnstile Area	95%	39%	94%	97%
Hybrone Test Room	100%	34%	100%	100%
Biges Office Room	88%	9%	93%	88%
Overall	94.79%	38.50%	95.46%	95.54%

Table 4. Comparative Analysis of ArcFace, OpenFace, Dlib and FaceNet for Recall in Different Environments

Environment	ArcFace	OpenFace	Exadel	Dlib
Biges Warehouse	100%	100%	100%	100%
Hybrone Turnstile Area	95%	62%	94%	98%
Hybrone Test Room	100%	23%	100%	100%
Biges Office Room	74%	26%	90%	87%
Overall	91.45%	51.49%	94.63%	96.12%

Table 5. Comparative Analysis of ArcFace, OpenFace, Dlib and FaceNet for F1 measure in Different Environments

Environment	ArcFace	OpenFace	Exadel	Dlib
Biges Warehouse	100%	100%	100%	100%
Hybrone Turnstile Area	95%	48%	94%	98%
Hybrone Test Room	100%	27%	100%	100%
Biges Office Room	77%	13%	89%	86%
Overall	92.16%	42.5%	94.39%	95.48%

The results of the test series show that the face recognition performance of the methods varies depending on environmental conditions and scenario types, as shown in Table 2. Exadel, Dlib, and ArcFace methods achieved 100% accuracy in controlled environments and less demanding scenarios, such as the Biges Warehouse and the Hybrone Test Chamber. However, OpenFace was only able to achieve full success on the Biges Warehouse dataset. Dlib (98.3%) showed higher accuracy than Exadel (93.4%) in the Hybrone Turnstile Area. ArcFace accuracy has decreased with more complex enviroments. This suggests that Dlib may be more resilient to more complex environmental factors and moving regions. Although Exadel (90.3%) achieved slightly higher accuracy than Dlib (87.1%) in the Biges Office Room, the performance of both methods decreased in this more challenging environment. Overall, Dlib achieved an accuracy of 96.1%, outperforming Exadel's overall accuracy of 94.6%. Although the ArcFace method achieved better results than the OpenFace method, it fell behind the other two methods.These results indicate that although Dlib generally performs better, it demonstrates greater resilience in certain complex scenarios. But OpenFace result Data Management Center (DMC) Alert was not triggered in any scenario, but different environments present different challenges.

Table 6. DMC Alarm State in Different Environments

Environment	ArcFace	OpenFace	Exadel	Dlib
Biges Warehouse	0	0	0	0
Hybrone Turnstile Area	1	0	0	0
Hybrone Test Room	0	0	0	0
Biges Office Room	7	4	0	0
Overall	8	4	0	0

As part of our system, we have a product called Data Monitoring Center (DMC), which is used by our alarm monitoring center. The inclusion of the DMC alarm status in Table 6 is critical due to its role in our security protocol. A DMC alarm is triggered when an unidentified person disarm security panel. This results in an automatic alarm being sent and our staff contacting the customer to inform them that an unidentified person has disarm the panel and the police are sent to the address. This means that the face recognition system misidentifies a known person as unknown, which can lead to significant security responses. Therefore, the inclusion of the DMC alarm in the table emphasizes the practical implications of misidentification by our facial recognition system and highlights the need for high accuracy to avoid false alarms and ensure reliable security measures. These results show that the Exadel and Dlib methods can be successful under ideal test conditions, but the OpenFace and ArcFace methods are not suitable.

5. Conclusion

The comparative analysis of the algorithms of Dlib and Exadel shows that both methods are very effective in face recognition tasks, especially in controlled environments. Dlib proved to be consistently more robust in more complex and dynamic environments, such as the Hybrone Turnstile Area. In contrast, Exadel FaceNet showed slightly higher accuracy in the Biges Office Room. Overall, the comparative evaluation shows that Exadel achieved a higher accuracy of 96.1%, while Dlib demonstrated a slightly lower overall accuracy of 94.6%, though Dlib proved to be more robust in complex environmental scenarios.

These results suggest that while both algorithms are suitable for high-accuracy face recognition, the choice of algorithm may depend on the specific challenges of the environment and the requirements of the application. The study highlights the importance of considering both algorithm performance and environmental factors when deploying facial recognition systems in real-world scenarios. Further research could investigate hybrid approaches that leverage the strengths of both methods to optimize performance under different conditions.

The practical applications of the results obtained from this study are significant and far-reaching. The comparative analysis of face recognition methods under different environmental conditions provides important insights for the use of these technologies in practice. The higher overall accuracy and robustness of Dlib in dynamic and complex scenarios suggest that it is suitable for environments such as public transportation hubs, surveillance in crowded areas, and dynamic office environments where variability and movement are prevalent. Conversely, Exadel's slightly better performance in controlled environments highlights its potential for secure access control in stable environments such as warehouses and test chambers.

Furthermore, the integration of these results into security systems such as our Data Monitoring Center (DMC) highlights the importance of reliable facial recognition to avoid false alarms and ensure a timely and accurate response to security breaches. By demonstrating that Dlib is generally more resilient in complex scenarios, organizations can make informed decisions about deploying this technology in highly sensitive environments, improving security measures and operational efficiency. This study highlights the need to select the appropriate facial recognition algorithm based on specific application needs and environmental challenges, ultimately contributing to the advancement and optimization of security systems worldwide.

Acknowledgment

We thank the Hybrone Team for providing the necessary resources and tireless support throughout this research. We are indebted to Çukurova University for their valuable insights and expertise. We owe special recognition to the developers and maintainers of the Dlib, Deepface, and Exadel projects, whose open source contributions greatly facilitated this work. We also thank the Biges participants who contributed to the dataset. Their collaboration contributed significantly to the successful completion of this study.

References

[1] Kortli, Y., Jridi, M., Al Falou, A., Atri, M. (2020). Face recognition systems: A survey. Sensors, 20(2), 342.

[2] Elngar, A. A., Kayed, M. (2020). Vehicle security systems using face recognition based on internet of things. Open Computer Science, 10(1), 17-29.

[3] Tribuana, D., Hazriani, H., Arda, A. L. (2024). Face recognition for smart door security access with convolutional neural network method. TELKOMNIKA (Telecommunication Computing Electronics and Control), 22(3), 702-710.

[4] Ben Fredj, H., Bouguezzi, S., Souani, C. (2021). Face recognition in unconstrained environment with CNN. The Visual Computer, 37(2), 217-226.

[5] Budiman, A., Yaputera, R. A., Achmad, S., Kurniawan, A. (2023). Student attendance with face recognition (LBPH or CNN): Systematic literature review. Procedia Computer Science, 216, 31-38.

[6] Li, L., Mu, X., Li, S., Peng, H. (2020). A review of face recognition technology. IEEE access, 8, 139110-139120.

[7] Geitgey, A. (n.d.). face_recognition. GitHub repository. Retrieved June 14, 2024, from https://github.com/ageitgey/face_recognition

[8] Exadel Inc. (n.d.). CompreFace. GitHub repository. Retrieved June 14, 2024, from https://github.com/exadel-inc/CompreFace

[9] Serengil, S., Özpınar, A. (2024). A Benchmark of Facial Recognition Pipelines and Co-Usability Performances of Modules. Bilişim Teknolojileri Dergisi, 17(2), 95-107.

[10] Komlavi, A. A., Chaibou, K., Naroua, H. (2022). Comparative study of machine learning algorithms for face recognition. Revue Africaine de Recherche En Informatique et Mathématiques Appliquées, 40.

[11] Radhika, C., Pathak, B. V. (2018). Face recognition based attendance system using machine learning algorithms. In 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS). ("2018 Second International Conference on Intelligent Computing and…"). IEEE.

[12] Güven, Ö. (2021). An Application on Identification With The Face Recognition System. Electronic Letters on Science and Engineering, 17(2), 198-207.

[13] Yakovleva, O., Kovtunenko, A., Liubchenko, V., Honcharenko, V., Kobylin, O. (2023). Face Detection for Video Surveillance-based Security System. In COLINS (3) (pp. 69-86).

[14] Mohammed, M. G., Melhum, A. I. (2020). Implementation of HOG feature extraction with tuned parameters for human face detection. International Journal of Machine Learning and Computing, 10(5), 654-661.

[15] Wu, C., Zhang, Y. (2021). MTCNN and FACENET based access control system for face detection and recognition. Automatic Control and Computer Sciences, 55, 102-112.

[16] Deng, J., Guo, J., Zhou, Y., Yu, J., Kotsia, I., Zafeiriou, S. (2019). Retinaface: Single-stage dense face localisation in the wild. arXiv preprint arXiv:1905.00641.

[17] Shi, Y., Yu, X., Sohn, K., Chandraker, M., Jain, A. K. (2020). Towards universal representation learning for deep face recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 6817-6826).

[18] Schroff, F., Kalenichenko, D., Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 815-823).

[19] Suwarno, S., & Kevin, K. (2020). Analysis of face recognition algorithm: Dlib and opencv. Journal of Informatics and Telecommunication Engineering, 4(1), 173-184.

[20] Baltrušaitis, T., Robinson, P., Morency, L. P. (2016, March). Openface: an open source facial behavior analysis toolkit. In 2016 IEEE winter conference on applications of computer vision (WACV) (pp. 1-10). IEEE.

[21] Deng, J., Guo, J., Xue, N., Zafeiriou, S. (2019). Arcface: Additive angular margin loss for deep face recognition. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 4690-4699).

[22] Malkauthekar, M. D. (2013, October). Analysis of euclidean distance and manhattan distance measure in face recognition. In Third International Conference on Computational Intelligence and Information Technology (CIIT 2013) (pp. 503-507). IET.

[23] Nguyen, H. V., Bai, L. (2010, November). Cosine similarity metric learning for face verification. In Asian conference on computer vision (pp. 709-720). Berlin, Heidelberg: Springer Berlin Heidelberg.