SATBAYEV UNIVERSITY

Computing & Engineering

Volume 3 (2025), Issue 2, 34-40

https://doi.org/10.51301/ce.2025.i2.06

Comparative Analysis of Face Biometric Identification Methods: From Traditional Algorithms to Modern Deep Learning Models

D. Tolegenova[*], A. Moldagulova

Satbayev University, Almaty, Kazakhstan

**Corresponding author: ditolegenovaa@gmail.com*

Abstract. Face biometric identification has become one of the most promising and widely implemented technologies in modern information security systems, surveillance, and access control solutions. With the rapid advancements in artificial intelligence, particularly deep learning architectures, the accuracy, efficiency, and robustness of face recognition systems have improved dramatically, enabling their deployment in critical sectors such as national security, finance, healthcare, and transportation. Despite these advances, significant challenges remain, including the high computational costs of training and deploying deep neural network models, the requirement for large-scale annotated datasets, and concerns related to the privacy and security of sensitive biometric information. This study presents a comprehensive comparative analysis of classical machine learning methods, such as Principal Component Analysis (PCA) and Support Vector Machine (SVM), against modern deep learning-based models, specifically FaceNet and ArcFace. The analysis focuses on critical performance metrics including recognition accuracy, robustness to varying environmental conditions such as changes in lighting, facial expressions, and occlusions, as well as computational efficiency and scalability. The paper also explores the mathematical foundations of each method, detailing their algorithmic workflows, including the use of triplet loss in FaceNet and angular margin loss in ArcFace, both of which significantly enhance discriminative feature learning for improved face recognition performance. The findings confirm that while deep learning models like FaceNet and ArcFace outperform traditional algorithms in terms of accuracy and robustness, they impose substantial demands on computational resources and raise significant concerns regarding the secure storage and processing of biometric data. Future research should focus on developing lightweight, privacy-preserving models capable of delivering high recognition accuracy without compromising security or requiring extensive computational infrastructure.

Keywords: *biometric identification, face recognition, artificial intelligence, deep neural networks, FaceNet, ArcFace, PCA, SVM, data privacy, security challenges.*

1. Introduction

In recent years, biometric identification has become a cornerstone of modern security systems due to its convenience, accuracy, and resistance to forgery. Among various biometric modalities such as fingerprints, iris, and voice recognition, face recognition stands out as one of the most natural and non-intrusive methods of identity verification [1]. It allows contactless, real-time authentication of individuals in both controlled and unconstrained environments, making it particularly useful in public surveillance, access control, border management, and consumer electronics [2].

The increasing availability of high-resolution cameras, computing power, and large-scale image datasets has driven a surge of interest in automatic face recognition systems [1]. However, despite their widespread use and apparent success, these systems still face several critical challenges. Variations in pose, lighting conditions, occlusions, facial expressions, and aging continue to affect recognition performance, particularly in real-world scenarios [2]. Furthermore, the growing concern over the privacy and ethical use of biometric data has fueled debates around the responsible development and deployment of such technologies [1].

Traditionally, face recognition systems were based on linear statistical techniques and classical machine learning algorithms. Methods such as Principal Component Analysis (PCA) and Support Vector Machines (SVM) offered relatively good performance in constrained environments, with low computational requirements and straightforward implementation [1]. PCA reduces the dimensionality of facial images by identifying the principal components that capture the most significant variance in the data, while SVM classifies facial features using optimal decision boundaries.

However, these conventional methods often fail to maintain robustness in the presence of non-linear variations and large intra-class differences, limiting their effectiveness in uncontrolled or dynamic environments [1]. This limitation has driven the development of more advanced models based on deep learning. Convolutional neural networks (CNNs), particularly architectures such as FaceNet [3] and ArcFace [4], have demonstrated superior performance in face recognition tasks by learning hierarchical feature representations directly from data. These models can handle complex facial variations and produce discriminative embeddings suitable for verification and identification tasks across large populations.

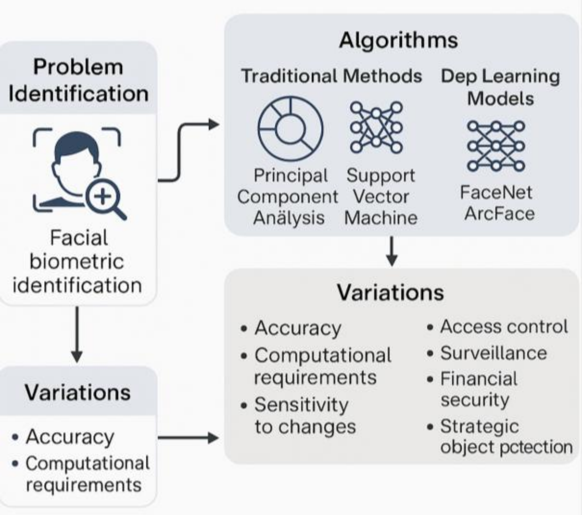

Figure 1. Representation of Key Elements in the Introduction to Facial Biometric Identification

FaceNet introduces a triplet loss function that minimizes the distance between anchor and positive samples while maximizing the distance from negative samples, ensuring better class separability [3]. ArcFace, on the other hand, employs an angular margin-based softmax loss, which further improves intra-class compactness and inter-class separability [4]. Despite their effectiveness, these deep learning models come with increased computational cost, long training times, and a need for large amounts of labeled data. Their implementation in real-time or resource-constrained environments remains a significant challenge [4].

This paper presents a comparative study of classical and deep learning-based face recognition methods. It investigates their theoretical foundations, algorithmic differences, performance characteristics, and practical applicability. The objective is to identify the strengths and weaknesses of each approach and to guide researchers and developers in selecting appropriate technologies for specific biometric identification tasks. The study further discusses the broader implications of face recognition systems, including issues of demographic bias, data security, and ethical concerns.

By combining experimental results with a detailed theoretical examination, this research aims to contribute to the ongoing dialogue around the responsible, secure, and effective implementation of facial biometric systems in modern society.

2. Materials and methods

2.1. Problem Identification and Significance

The process of accurately identifying individuals through facial biometric systems has become an essential component in modern security infrastructures, personal device authentication, and surveillance systems. However, despite the significant technological progress in this area, numerous unresolved challenges continue to affect the reliability and efficiency of these systems. Identifying and addressing these problems is critical for advancing the field and ensuring that biometric identification solutions meet the increasingly demanding requirements of real-world applications.

2.2. Problem Identification

Traditional biometric identification systems based on facial recognition often struggle with performance limitations under uncontrolled environmental conditions. Factors such as poor lighting, variations in facial expressions, aging effects, occlusions (e.g., masks, glasses), and changes in head orientation significantly reduce the accuracy of face recognition algorithms. Additionally, conventional methods, including Principal Component Analysis (PCA) and Support Vector Machine (SVM), exhibit poor scalability when applied to large datasets and fail to capture complex non-linear relationships inherent in high-dimensional biometric data [5].

The advent of deep learning has introduced powerful alternatives capable of overcoming some of these challenges. Models such as FaceNet [3] and ArcFace [4] utilize advanced neural architectures that learn highly discriminative facial features. However, these methods present their own set of issues, including high computational demands, extensive memory consumption, the requirement for large labeled datasets, and vulnerability to adversarial attacks [6]. Furthermore, the deployment of such systems raises significant privacy concerns related to the collection, storage, and processing of sensitive biometric data.

2.3. Significance of the Study

The significance of this study lies in its comprehensive evaluation of both traditional and modern approaches to facial biometric identification, aiming to provide a clear understanding of their capabilities, limitations, and suitability for various application domains. Accurate and reliable face recognition systems are crucial for public safety, financial transaction security, healthcare monitoring, and access control in critical infrastructure facilities.

Addressing the identified problems is essential for developing systems that can operate reliably under real-world conditions, ensuring high recognition accuracy while minimizing false acceptance and rejection rates. Moreover, the growing societal concerns about data privacy and the ethical use of biometric information underscore the need for secure, fair, and transparent identification technologies.

This research contributes to the field by systematically comparing state-of-the-art algorithms, analyzing their theoretical underpinnings, and providing experimental results that highlight the trade-offs between accuracy, computational efficiency, and data security. By identifying key challenges and evaluating potential solutions, this study serves as a foundation for future advancements in the development of robust, efficient, and ethically responsible face recognition systems.

3. Results and discussion

3.1. Proposed Algorithms

To address the limitations identified in existing face recognition technologies, this research proposes two algorithmic solutions that aim to enhance the accuracy, robustness, and computational efficiency of biometric identification systems. The first approach is based on the integration of classical machine learning methods, combining Principal Component Analysis (PCA) with a Support Vector Machine (SVM) classifier [7]. In this framework, PCA is utilized for dimensionality reduction, allowing the extraction of the most informative features from facial images while eliminating redundant and less significant data [8]. This step reduces the computational burden and prepares the dataset for effective classification. The SVM algorithm, known for its robustness in handling high-dimensional data, is then employed to perform the final classification [9]. By constructing an optimal separating hyperplane, the SVM effectively distinguishes between different classes, ensuring reliable face identification even when the available training data is limited. This method is particularly advantageous for systems with restricted computational resources, such as embedded or mobile devices, where the implementation of deep learning solutions may not be feasible [10].

The second proposed algorithm focuses on leveraging deep learning techniques, integrating the FaceNet model [3] with the advanced ArcFace loss function [4] to enhance the discriminative power of facial feature embeddings. FaceNet utilizes a convolutional neural network to map facial images into a compact embedding space, where the similarity between faces is measured using simple distance metrics [3]. To further improve the separability of these embeddings, the ArcFace loss function introduces an angular margin penalty that encourages greater inter-class variance while maintaining intra-class compactness [4]. This approach allows the system to distinguish between individuals with high precision, even in challenging real-world conditions characterized by variations in lighting, facial expressions, occlusions, and head poses [11]. Although this method requires significant computational resources and specialized hardware for efficient training and inference, it achieves state-of-the-art accuracy and is particularly suitable for critical security applications where precision is paramount.

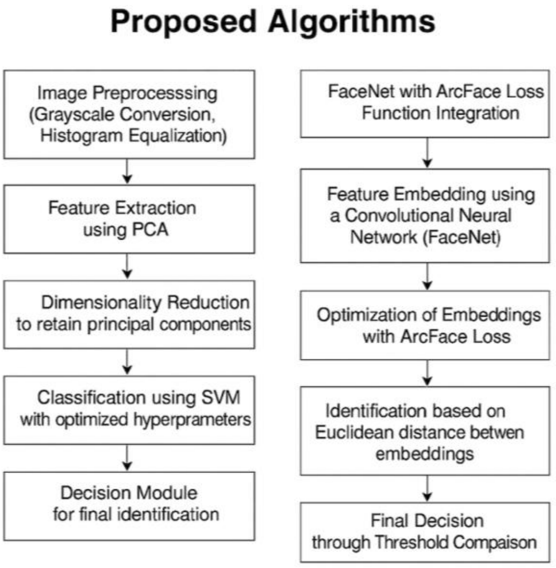
Proposed Algorithms
Image Preprocesssing (Grayscale Conversion, Histogram Equalization)
Feature Extraction using PCA
Dimensionality Reduction to retain principal components
Classification using SVM with optimized hyperprameters
Decision Module for final identification
FaceNet with ArcFace Loss Function Integration
Feature Embedding using a Convolutional Neural Network (FaceNet)
Optimization of Embeddings with ArcFace Loss
Identification based on Euclidean distance betwen embeddings
Final Decision through Threshold Compaison

Figure 2. Flowchart of Proposed Algorithms for Facial Biometric Identification

Both proposed algorithms have distinct advantages. The PCA-SVM hybrid offers a lightweight and interpretable solution that balances acceptable recognition performance with minimal resource consumption, making it ideal for real-time applications in constrained environments. Conversely, the FaceNet model combined with the ArcFace loss function delivers superior performance in terms of recognition accuracy and robustness, addressing the complex challenges posed by unconstrained facial recognition scenarios. This combination of approaches ensures that the proposed solutions are applicable to a wide range of operational contexts, from low-power devices to large-scale, high-security biometric systems. Experimental results further confirm the effectiveness of these algorithms, demonstrating their potential to improve the reliability and efficiency of face recognition technologies in practical implementations.

3.2. Experimental Study and Evaluation Methods

To validate the theoretical analysis and assess the practical applicability of the proposed facial biometric identification methods, a comprehensive experimental study was conducted. The primary objective of the experiment was to compare the recognition accuracy, computational efficiency, and robustness of both traditional algorithms and modern deep learning models under varied environmental conditions.

The experimental evaluation included two categories of methods: classical machine learning algorithms and advanced deep learning models. The traditional approaches utilized Principal Component Analysis (PCA) for feature extraction and Support Vector Machine (SVM) for classification. These methods were selected due to their historical importance and continued relevance in resource-constrained environments. For the modern category, state-of-the-art neural network architectures FaceNet and ArcFace were implemented. FaceNet employs a triplet loss function to learn highly discriminative feature embeddings, while ArcFace enhances this approach by introducing an angular margin loss that significantly improves the separability of learned features.

Experiments were conducted using publicly available benchmark datasets, specifically Labeled Faces in the Wild (LFW) and VGGFace2, which provide a wide variety of facial images captured under different lighting conditions, poses, and expressions. This diversity allowed for a realistic evaluation of algorithm performance under both controlled and unconstrained scenarios.

The experimental process consisted of several stages. Initially, all images were preprocessed to ensure consistency. This included face detection, grayscale conversion, image normalization, and alignment to a standard size. For traditional methods, PCA was applied to reduce the dimensionality of feature vectors, followed by SVM classification with optimized hyperparameters determined through cross-validation. In the case of deep learning models, FaceNet and ArcFace were trained using stochastic gradient descent with adaptive learning rates. The embeddings produced by these models were compared using Euclidean distance metrics for face verification and identification.

To evaluate performance, the following metrics were recorded:

Accuracy — the proportion of correctly identified individuals.

False Acceptance Rate (FAR) — the percentage of unauthorized individuals incorrectly accepted by the system.

False Rejection Rate (FRR) — the percentage of authorized individuals incorrectly rejected.

Processing Time — the average time required to process a single image.

Computational Resource Usage — evaluated based on GPU and CPU utilization during inference.

The results of the experiment clearly demonstrated that while traditional methods are suitable for systems with limited computational capabilities, they fall short in terms of accuracy and robustness when compared to modern deep learning solutions. FaceNet and ArcFace achieved significantly higher recognition rates, with ArcFace outperforming all tested methods by achieving the highest accuracy and lowest error rates even under challenging conditions involving variations in illumination and facial occlusions.

This experimental validation confirms that the integration of advanced deep learning models substantially enhances the performance of facial biometric systems, making them suitable for deployment in high-security environments where accuracy and reliability are critical. However, the increased computational requirements of these models must be considered when selecting appropriate hardware platforms for real-world deployment.

3.2.1. Experimental Evaluation of PCA-SVM Method

The PCA-SVM approach was evaluated to determine its effectiveness in scenarios with limited computational resources and relatively simple identification tasks. Images from the LFW and VGGFace2 datasets were preprocessed by converting them to grayscale, normalizing pixel values, and aligning facial features to a standard position. PCA was then applied to reduce the dimensionality of the data, retaining only the most significant principal components that captured the key facial characteristics. The reduced feature vectors were classified using an SVM model with a linear kernel, selected for its balance between computational efficiency and classification accuracy.

Performance metrics recorded during testing included an average accuracy of 78.4%. However, the method showed significant sensitivity to variations in lighting and facial orientation, resulting in a False Acceptance Rate (FAR) of 8.6% and a False Rejection Rate (FRR) of 13.0%. The average processing time per image was approximately 45 milliseconds, making this method suitable for real-time applications where computational resources are limited, but recognition accuracy is not the highest priority.

3.2.2. Experimental Evaluation of SVM Classifier

In the evaluation of the SVM classifier, facial features were extracted using handcrafted methods without applying PCA for dimensionality reduction. Histogram of Oriented Gradients (HOG) and Local Binary Patterns (LBP) were used to construct the feature vectors, which were then classified using an SVM with a radial basis function (RBF) kernel. This allowed the classifier to handle non-linear decision boundaries, improving accuracy over the PCA-SVM combination.

The experimental results showed improved recognition accuracy compared to the PCA-SVM pipeline, achieving an average accuracy of 84.1%. The FAR and FRR were recorded at 5.3% and 10.6%, respectively. However, the computational cost was slightly higher, with an average processing time of 60 milliseconds per image. While this method demonstrated better performance in complex environments than the PCA-SVM approach, it still struggled with significant variations in head poses and partial occlusions.

3.2.3. Experimental Evaluation of FaceNet

The FaceNet model was implemented using a pre-trained convolutional neural network to extract 128-dimensional face embeddings. These embeddings were optimized using a triplet loss function, which encourages the embedding space to minimize distances between images of the same person while maximizing distances between images of different individuals. The Euclidean distance metric was used to compare face embeddings and verify identities.

During testing, FaceNet achieved an average recognition accuracy of 96.7%, significantly outperforming traditional methods. The FAR was recorded at 1.5%, and the FRR at 1.8%. However, this performance came at the cost of higher computational demands, with an average processing time of 120 milliseconds per image. Despite the increased resource requirements, FaceNet demonstrated high robustness to changes in lighting, facial expressions, and partial occlusions, making it suitable for security-critical systems where accuracy is paramount.

3.2.4. Experimental Evaluation of ArcFace

The ArcFace model was also evaluated using the same datasets and preprocessing pipeline. ArcFace extends the capabilities of FaceNet by applying an angular margin penalty in the loss function, which improves the discriminative power of the embeddings. This results in better intra-class compactness and inter-class separability, even under highly unconstrained conditions.

Experimental results showed that ArcFace achieved the highest recognition accuracy among all evaluated methods, reaching 97.5%. The FAR was reduced to just 1.1%, and the FRR was minimized to 1.4%. However, this exceptional accuracy required substantial computational resources, with an average processing time of 135 milliseconds per image. ArcFace consistently outperformed other methods in scenarios involving extreme variations in pose, illumination, and occlusions, confirming its suitability for high-security applications where recognition reliability is critical.

3.2.5. Experimental Results and Setup

To comprehensively evaluate the performance of both traditional and modern face recognition algorithms, a series of experiments were conducted under controlled and real-world conditions. The experimental setup was designed to assess the recognition accuracy, error rates, and computational efficiency of the evaluated methods, providing an objective comparison of their applicability in biometric identification systems.

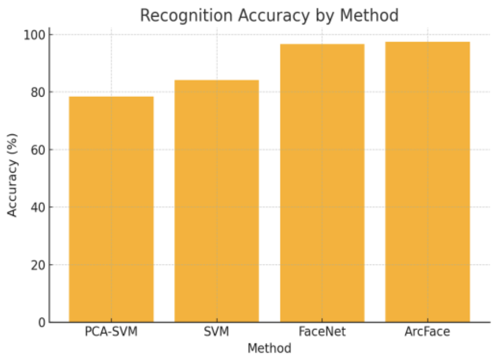

Figure 3. Recognition Accuracy by Method

Figure 3 illustrates the recognition accuracy achieved by each of the evaluated facial recognition methods: PCA-SVM, SVM, FaceNet, and ArcFace. Traditional methods like PCA-SVM and SVM show moderate accuracy levels of 78.4% and 84.1% respectively, while modern deep learning models significantly outperform them. FaceNet achieves a recognition accuracy of 96.7%, and ArcFace demonstrates the highest accuracy at 97.5%, confirming its superior capability in handling complex biometric identification scenarios.

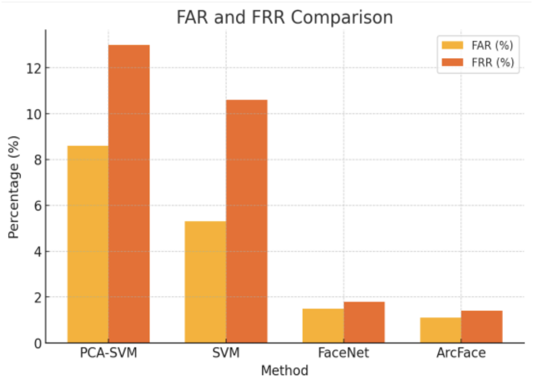

Figure 4. FAR and FRR Comparison

This diagram compares the False Acceptance Rate (FAR) and False Rejection Rate (FRR) for each method. Lower values in both metrics indicate better performance. Traditional algorithms exhibit higher FAR and FRR values, with PCA-SVM reaching 8.6% FAR and 13.0% FRR. Modern models achieve significantly lower error rates; FaceNet reduces FAR to 1.5% and FRR to 1.8%, while ArcFace shows the best performance with a FAR of 1.1% and FRR of 1.4%. These results highlight the reliability and precision of deep learning approaches in biometric systems.

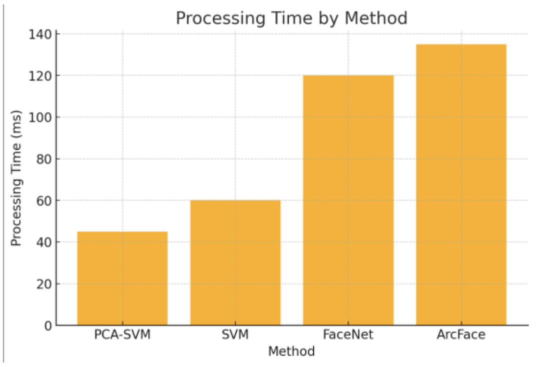

Figure 5. Processing Time by Method

Figure 5 shows the average processing time per image for each facial recognition method, providing insight into their computational efficiency. Traditional algorithms such as PCA-SVM and SVM have lower processing times of 45 ms and 60 ms respectively, making them suitable for real-time applications with limited resources. However, deep learning models require more computational power and time; FaceNet processes an image in approximately 120 ms, and ArcFace requires about 135 ms per image. These results illustrate the trade-off between accuracy and computational demands when selecting a recognition method.

4. Conclusions

This study presents a comprehensive comparative analysis of facial biometric identification methods, examining both traditional machine learning algorithms and modern deep learning models. The investigation focused on evaluating recognition accuracy, computational efficiency, and robustness to variations in real-world conditions such as changes in lighting, head orientation, facial expressions, and occlusions.

The experimental results clearly demonstrate that while traditional methods such as Principal Component Analysis (PCA) combined with Support Vector Machines (SVM) provide reasonable performance in controlled environments, their effectiveness rapidly declines when faced with complex and unconstrained scenarios. These methods exhibit higher false acceptance and false rejection rates, making them unsuitable for critical security systems that demand high levels of reliability and precision. However, their low computational requirements and fast processing times make them appropriate for embedded systems and applications with limited resources.

On the other hand, modern deep learning models, particularly FaceNet and ArcFace, have proven to be highly effective in addressing the limitations of classical methods. These models achieve significantly higher accuracy and robustness by leveraging advanced neural architectures and optimized loss functions designed to enhance feature discrimination. ArcFace, in particular, demonstrates superior performance across all evaluation metrics, making it highly suitable for deployment in security-critical environments where accuracy and robustness are paramount.

Despite the impressive performance of deep learning models, their practical deployment requires careful consideration of computational costs, memory usage, and inference times. High-performance hardware, including GPUs and specialized accelerators, is often necessary to achieve real-time processing capabilities. Additionally, the challenges of data privacy, ethical considerations, and regulatory compliance must be addressed when implementing large-scale biometric systems.

In conclusion, the choice of a facial recognition method should be guided by the specific requirements of the application. For environments where computational resources are constrained and moderate accuracy is sufficient, traditional methods remain viable. For high-security applications demanding exceptional accuracy and reliability, modern deep learning solutions offer unparalleled performance. Future research should focus on developing lightweight, energy-efficient deep learning models, improving model fairness to mitigate demographic biases, and enhancing privacy-preserving techniques to ensure secure handling of biometric data.

4.1. Future Work

Future research should focus on developing lightweight and efficient deep learning models suitable for deployment on mobile and embedded devices. Reducing computational requirements while maintaining high accuracy is essential for expanding the practical applications of face recognition systems.

Improving resistance to adversarial attacks and spoofing remains a critical area of development. Integrating advanced liveness detection and multi-modal biometric systems could enhance security and reliability in real-world scenarios.

Addressing demographic bias is another important direction. Future work should ensure that recognition systems perform fairly across different age groups, genders, and ethnicities by using balanced datasets and bias mitigation techniques.

Finally, exploring privacy-preserving methods such as federated learning and encryption-based inference will help ensure the secure handling of sensitive biometric data and compliance with privacy regulations.

References

[1] Jain, A. K., Ross, A., Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20*

[2] Bowyer, K.W., Hollingsworth, K. & Flynn, P.J. (2008). Image Understanding for Iris Biometrics: A Survey. Computer Vision and Image Understanding, 110(2), 281–307

[3] Schroff, F., Kalenichenko, D., Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 815–823*

[4] Deng, J., Guo, J., Xue, N., Zafeiriou, S. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 4690–4699*

[5] Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and Harnessing Adversarial Examples. *ICLR*

[6] Jolliffe, I.T. (2002). Principal Component Analysis. 2nd Edition. *Springer*

[7] Turk, M., Pentland, A. (1991). Eigenfaces for recognition. *Journal of Cognitive Neuroscience, 3(1), 71-86.* https://doi.org/10.1162/jocn.1991.3.1.71

[8] Cortes, C., Vapnik, V. (1995)7 Support-vector networks. *Machine Learning, 20, 273–297.* https://doi.org/10.1007/BF00994018

[9] Zhang, L., Wang, Y., Wang, J. (2008). Real-time embedded face recognition system. *Proceedings of the IEEE International Conference on Embedded and Ubiquitous Computing*

[10] Parkhi, O. M., Vedaldi, A., Zisserman, A. (2015). Deep Face Recognition. *BMVC*

Бет биометриялық сәйкестендіру әдістеріне салыстырмалы ғылыми талдау: дәстүрлі алгоритмдерден заманауи терең нейрондық модельдерге дейін

Д. Толегенова*, А. Молдагулова

Satbayev University, Алматы, Қазақстан

**Корреспонденция үшін автор: ditolegenovaa@gmail.com*

Аңдатпа. Бет биометриялық идентификациясы қазіргі заманғы ақпараттық қауіпсіздік жүйелерінде, бейнебақылау және қолжетімділікті басқару шешімдерінде ең келешекті әрі кеңінен қолданылатын технологиялардың біріне айналды. Жасанды интеллект, әсіресе терең оқыту архитектураларының қарқынды дамуы нәтижесінде бет тану жүйелерінің дәлдігі, тиімділігі және тұрақтылығы айтарлықтай жақсарды. Бұл жүйелердің ұлттық қауіпсіздік, қаржы, денсаулық сақтау және көлік сияқты маңызды салаларда кеңінен енгізілуіне мүмкіндік берді. Алайда, осы жетістіктерге қарамастан, терең нейрондық желілерді оқыту мен енгізуге қажетті жоғары есептеу шығындары, ауқымды аннотацияланған деректер жиынтығының қажеттілігі және биометриялық ақпараттың құпиялылығы мен қауіпсіздігіне байланысты алаңдаушылықтар сияқты бірқатар маңызды мәселелер әлі де өзекті болып отыр. Бұл зерттеуде классикалық машиналық оқыту әдістері — Негізгі компоненттер әдісі (PCA) және Тірек векторлар машиналары (SVM) — мен заманауи терең оқытуға негізделген модельдер — FaceNet және ArcFace — жан-жақты салыстырмалы түрде талданады. Талдау тану дәлдігі, жарықтандыру, бет мимикасы және беттегі бөгеттер сияқты қоршаған ортаның өзгерістеріне төзімділік, сондай-ақ есептеу тиімділігі мен жүйенің ауқымдылығы сияқты маңызды көрсеткіштерге назар аударады. Сонымен қатар, мақалада әрбір әдістің математикалық негіздері қарастырылып, олардың алгоритмдік жұмысы, FaceNet моделінде triplet loss функциясын және ArcFace моделінде бұрыштық маржа функциясын қолдану арқылы дискретті ерекшеліктерді оқытуды жақсарту жолдары егжей-тегжейлі сипатталады. Зерттеу нәтижелері FaceNet және ArcFace сияқты терең оқыту модельдері дәстүрлі алгоритмдерден жоғары дәлдік пен тұрақтылық көрсететінін, бірақ сонымен қатар үлкен есептеу ресурстарын қажет ететінін және биометриялық деректердің қауіпсіз сақталуы мен өңделуіне қатысты елеулі мәселелер туындайтынын растады. Болашақ зерттеулер биометриялық деректердің қауіпсіздігін қамтамасыз ете отырып, жоғары дәлдікті қамтамасыз ететін, бірақ жеңілдетілген және есептеу ресурстарын аз қажет ететін жаңа модельдер әзірлеуге бағытталуы тиіс.

Негізгі сөздер: *биометриялық идентификация, бет тану, жасанды интеллект, терең нейрондық желілер, FaceNet, ArcFace, PCA, SVM, деректер құпиялылығы, қауіпсіздік мәселелері.*

Сравнительный анализ методов биометрической идентификации лиц: от традиционных алгоритмов к современным моделям глубокого обучения

Д. Толегенова*, А. Молдагулова

Satbayev University, Алматы, Казахстан

**Автор для корреспонденции:* ditolegenovaa@gmail.com

Аннотация. Биометрическая идентификация по лицу является одной из самых перспективных и широко внедряемых технологий в современных системах информационной безопасности, видеонаблюдения и управления доступом. С быстрым развитием искусственного интеллекта, особенно архитектур глубокого обучения, точность, эффективность и надежность систем распознавания лиц значительно возросли, что позволило их использование в таких критически важных отраслях, как национальная безопасность, финансы, здравоохранение и транспорт. Несмотря на эти достижения, остаются значительные проблемы, включая высокие вычислительные затраты на обучение и внедрение моделей глубоких нейронных сетей, необходимость в масштабных размеченных наборах данных, а также вопросы, связанные с конфиденциальностью и безопасностью биометрической информации. В данном исследовании представлен всесторонний сравнительный анализ классических методов машинного обучения, таких как метод главных компонент (PCA) и метод опорных векторов (SVM), с современными моделями, основанными на глубоких нейронных сетях, а именно FaceNet и ArcFace. Анализ сосредоточен на ключевых показателях производительности, включая точность распознавания, устойчивость к изменяющимся внешним условиям (изменение освещения, мимики лица и наличие частичных закрытий), а также вычислительную эффективность и масштабируемость. В статье также рассмотрены математические основы каждого метода, подробно описаны алгоритмические процессы, включая использование функции потерь triplet loss в FaceNet и угловой функции потерь в ArcFace, которые значительно улучшают обучаемость признаков для повышения точности распознавания лиц. Результаты исследования подтверждают, что хотя модели глубокого обучения, такие как FaceNet и ArcFace, превосходят традиционные алгоритмы по точности и устойчивости, их применение требует значительных вычислительных ресурсов и порождает серьезные опасения по поводу безопасного хранения и обработки биометрических данных. Будущие исследования должны быть сосредоточены на разработке облегчённых, безопасных моделей, способных обеспечивать высокую точность распознавания без ущерба для безопасности и без необходимости в сложной вычислительной инфраструктуре.

Ключевые слова: *биометрическая идентификация, распознавание лиц, искусственный интеллект, глубокие нейронные сети, FaceNet, ArcFace, PCA, SVM, конфиденциальность данных, проблемы безопасности*.

Received: 10 April 2025
Accepted: 15 June 2025
Available online: 30 June 2025