https://doi.org/10.53656/adpe-2025.15

ARTIFICIAL INTELLIGENCE AND BIOMETRIC TECHNOLOGIES IN DEFENSE: ALGORITHMS AND CHALLENGES

Radoslav Chalakov,
Andon Andonov,
Viara Jekova
Rakovski National Defence College, Sofia, Bulgaria

Abstract. Human resource management in defense is crucial for the efficiency, security, and readiness of military organizations. Emerging biometric recognition technologies and their application in defense HR management, facilitated by artificial intelligence (AI), play a pivotal role in advancing biometric identification systems. These systems incorporate technologies such as fingerprint recognition, facial recognition, iris scanning, and voice identification. When combined with AI-driven algorithms, they enhance the accuracy and efficiency of biometric data analysis and processing.

This paper examines the mathematical algorithms underpinning the identification process, including support vector machines (SVM), deep neural networks (DNN), and biometric feature extraction methods. Special emphasis is placed on the challenges associated with implementing such technologies in the defense sector, encompassing ethical and legal considerations related to personal data protection.

Keywords: Artificial intelligence; biometric data; human resource management; deep neural networks; support vector machines (SVM); identification and verification

1. Introduction

The advancement of artificial intelligence (AI) and machine learning technologies has led to the widespread adoption of biometric identification systems across various domains, including defense. The use of biometric data – such as fingerprints, facial recognition, and voice identification – enables enhanced security and efficiency in human resource management. The core focus of developing a biometric data analysis system for identity recognition in the defense sector revolves around the collection, processing, storage, and analysis of biometric information to authenticate and verify personnel.

The development of an AI-driven biometric recognition system for defense HR management involves multiple stages: data acquisition, processing, analysis, and feature recognition. The algorithm outlined below provides a structured approach to implementation. (Sokolova & Konushin, 2019).

1.1. Phase 1: Biometric Data Collection

The first phase involves gathering biometric data from personnel for identification and verification purposes. **The data collection algorithm includes:**

● *System Initialization:* Activation of cameras, scanners, and microphones, and support for multi-source data capture (e.g., simultaneous facial and fingerprint recording).

New Employee Enrollment: Identity validation of new personnel, biometric data capture using specialized devices; secure storage in an encrypted centralized database.

● *Data Quality Assurance:* Image clarity checks (e.g., lighting adjustments), noise and artifact detection in voice recordings, plus validation of fingerprint data accuracy and consistency.

1.2. Phase 2: Data processing and storage

Post-collection, biometric data undergoes preprocessing and secure storage with privacy safeguards. The processing algorithm comprises**:**

● *Image preprocessing:* Quality enhancement (e.g., noise reduction, lighting correction) and standardization of facial images for downstream analysis.

● *Voice Data Normalization:* Conversion to standardized audio formats (e.g. WAV, MP3) plus background noise suppression and amplitude normalization.

● *Data Encryption & Anonymization:* Encryption of biometric templates to protect sensitive information. In addition, hashing or anonymization techniques for GDPR compliance. Anonymization process refers to any particular record or set of data which has been made anonymous in a way that a certain individual cannot be identified or can no longer be identified by reasonably expected means. Hashing process generates a fixed-size output from variable-size input data. This is done by using mathematical hash functions (implemented as hashing algorithms).

● *Secure Data Storage:* High-security centralized databases (SQL/NoSQL for scalability); data redundancy to prevent loss.

1.3. Phase 3: Biometric data recognition and verification

This is the core stage in which biometric data recognition is performed by AI algorithms. The recognition algorithms must be trained and fine-tuned for biometric matching:

● *Model Initialization:* Selection of AI architectures (e.g., CNN for facial recognition, RNN or GMM for voiceprints) followed by training with pre-collected datasets to optimize accuracy.

● *Real-Time Data Processing:* Capturing of new biometric data in real time and standardization of the new biometric inputs.

● *Database matching:* Feature vector comparison using distance metrics (e.g., cosine/ Euclidean distance); threshold-based authentication also called match/ no-match decision.

● *Anomaly Detection:* Identification of spoofing attempts or outliers via anomaly detection algorithms supplemented by triggering secondary verification or alerts for suspicious activity.

● *Access Control:* If database match is successful, the system grants access to the resource or piece of information. Otherwise, if no match or an anomaly is detected, the access is denied and corresponding authorities notified for verification.

1.4. Phase 4: User Interface & Reporting

Role-specific interfaces enable system interaction**:**

● *Employee Portal:* Authentication dashboard with task/ attendance tracking.

● *Admin Console:* Access to biometric databases, audit logs, and analytics. Compliance reporting and anomaly visualization.

● *Real-time monitoring:* Live tracking of personnel access/ egress followed by attendance analytics for resource optimization.

1.5. Phase 5: AI Model Training

Continuous learning ensures sustained accuracy**:**

● *Training Data Aggregation:* Large-scale datasets with diverse biometric samples.

● *Machine Learning Optimization:* Model fine-tuning via deep neural networks (e.g., CNN, RNN).

● *Accuracy Validation:* Periodic testing with unseen data plus incremental learning to adapt to new biometric patterns.

2. Methodology

A. Mathematical algorithm of a biometric data recognition system in defence human resources management

The biometric recognition system through data analysis in defense human resource management aims to provide security and efficiency in identifying military personnel, as well as in access control and activity monitoring. This system must include several main stages: collection and processing of biometric data, feature extraction, model training, recognition and verification.

The algorithm for developing a recognition system through biometric data analysis in the context of defense human resource management is a multi-component task that involves processing biometric data, extracting their features, and using machine learning for personnel identification and verification. This requires high security, accuracy and speed. The system must ensure effective management of employee identification data through various biometric technologies (fingerprints, facial recognition, iris recognition, etc.).

In the present context, the underlying mathematical algorithm governing access acquisition may be formally characterized by the subsequent procedural phases (Alamdari & Krovi, 2016):

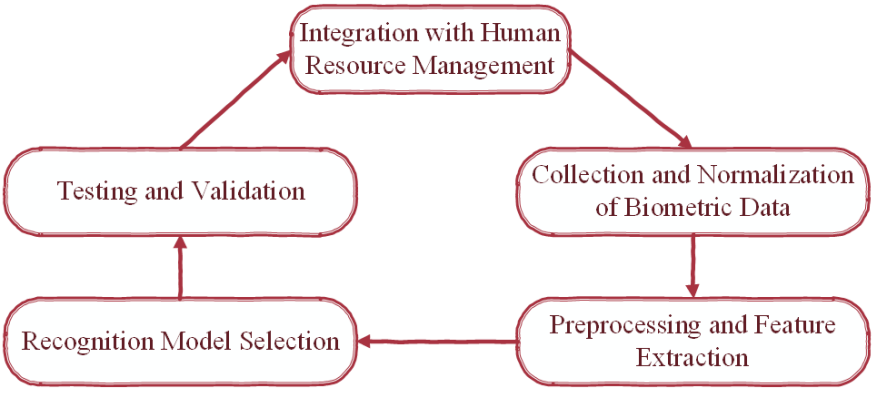

Figure 1. Mathematical algorithm model for gaining access

a. Biometric data collection and normalization

Biometric data in this case may include fingerprints, facial images, or other types of biometric data. Each employee in the system is associated with one or more biometric templates.

● **Biometric data collection –** for the aims of this analysis, let us consider two types of biometric data: X_{finger} – fingerprint biometric data (e.g., a vector containing information about unique point characteristics of fingerprints). X_{face} – facial images that contain important features such as the location of the eyes, nose, mouth, and facial contours.

● **Data normalization –** for its processing, the system data must be normalized. Normalization is performed to standardize data dimensions or to vectorize images into uniform dimensional representations.

$$X_{norm} = \frac{X_{raw} - \mu}{\sigma}, \tag{1}$$

where: X_{raw} – original dataset, μ – mean of the dataset, σ – standard deviation.

b. Preprocessing and feature extraction

Following data normalization, it is necessary to extract significant features that will be used for face or fingerprint identification.

● **Feature extraction –** for *fingerprints*, techniques such as *minutiae extraction* (unique fingerprint ridge characteristics) can be used. For *facial recognition*, distinctive facial features are extracted, including distances between eyes, ears, and contours of the nose and mouth.

● **Fingerprint Processing –** algorithms for *minutiae extraction* are applied to

fingerprint images. Let the fingerprint features be represented by the vector V_{finger} . (Grizhebovskaya & Mikhalev, 2019).

● **Facial Recognition** – *Principal Component Analysis (PCA)* or *Deep Convolutional Networks (CNN)* are used to extract distinctive facial features. After applying PCA or CNN to a facial image, a feature vector V_{face} is obtained:

$$V_{face} = PCA(X_{face}) \text{ or } V_{face} = CNN(X_{face}) \tag{2}$$

c. Recognition model selection

For personnel recognition and identification in defense systems, we employ machine learning algorithms such as **Support Vector Machines (SVM)** and **Deep Neural Networks (DNN)**. These models will be trained using the features extracted from employees' biometric data.

● **Model training** – let $X_{train} = \{V_{finger}, V_{face}\}$ be the training dataset, and $Y_{train} = \{y_1, y_2, \cdots y_N\}$ contain the corresponding employee identification data (labels). The model training aims to minimize the error between predicted and actual values.

Support vector machine (SVM) optimization objective would be:

$$L_{SVM} = \sum_{i=1}^{N} \max(0.1 - y_i f(X_i)) + \lambda \|\omega\|^2 , \tag{3}$$

where: y_i – true label of the employee, $f(X_i) = \omega^T X_i + b$ – model's predicted value, ω – vector of weighting factors, b – bias term, and λ – regularization parameter.

Deep neural network (DNN) training is performed by optimizing a loss function (e.g., cross-entropy loss):

$$L_{DNN} = -\sum_{i=1}^{N} (y_i \log(\hat{y}_i) + (1 - y_i) \log(1 - \hat{y}_i)) , \tag{4}$$

where $\hat{y}_i$ – represents the model's predicted probability distribution for classification.

d. Test and Validation

Following model training, the system must be tested and validated using new (unseen) biometric data to evaluate model performance.

● **Evaluation Metrics**

Accuracy – measures the overall correctness of the model:

$$Accuracy = \frac{Number\ of\ correctly\ classified\ examples}{Total\ number\ of\ examples} \quad (5)$$

Precision – indicates the proportion of true positives among all positive predictions:

$$Precision = \frac{True\ positives}{True\ positives + False\ positives} \quad (6)$$

Recall (Sensitivity) – measures the model's ability to detect all positive instances:

$$Recall = \frac{True\ positives}{True\ positives + False\ negatives} \quad (7)$$

Coefficient of correspondence (F1-Score) – harmonic mean of precision and recall, balancing both metrics:

$$F_1 = 2.\frac{Precision.Recall}{Precision + Recall} \quad (8)$$

e. Integration with Defence Human Resources Management

Once the model is trained and evaluated, it has to be integrated within the defense human resource management database. This integration involves the following key processes:

1) New employee registration involves recording of new employees' biometric data in the database. After that the system processes this data and links the extracted features with the employee's unique identifier in the system.

2) Recognition and verification. When an employee requests access to a restricted area or system their biometric data is captured in real-time and compared against stored templates in the database. Based on that, the recognition/ verification algorithm makes an access decision.

3) New biometric data processing. After the model is trained, the new biometric data x_{new} is fed to the model, which is supposed to predict the identity of the person. Feature extraction for new data:

$$x^*_{new} = PCA(x_{new}) \quad (9)$$

Identity prediction when using SVM is performed by calculating:

$$\hat{y}_{new} = SVM(x^*_{new}) \quad (10)$$

and when using a neural network:

$$\hat{y}_{new} = NN(x^{*}_{new}) \quad (11)$$

4) Access Control Verification – indicator of the difference between the new and old biometric characteristics should be defined by:

$$d(x_{new}, x_{stored}) = \|x_{new} - x_{stored}\|^2 \quad (12)$$

If the difference is less than a predefined threshold t, then the identification is successful:

$$d(x_{new}, x_{stored}) < t \Rightarrow successful\ verification \quad (13)$$

5) Verification – it is necessary to check whether the distance between the current biometric scan and storage is within acceptable limits, i.e. (Prudnik et al., 2014)

$$\hat{y}_{new} = SVM\,(x_{new}) \text{и}\ d(x_{new}, x_{stored}) < t \quad (14)$$

If these conditions are satisfied, access is granted.

3. Challenges

The development and implementation of an AI-powered biometric recognition system for defense human resource management entails a multifaceted process with significant technical, ethical, legal, and operational challenges (Patel & Gera, 2024).

Technical challenges include ensuring high accuracy and reliability in recognition algorithms to minimize false positives/ negatives – especially critical in military environments – alongside the need for robust big data processing capabilities to handle vast biometric datasets. Additionally, stringent cybersecurity measures are essential to protect sensitive biometric data from breaches, while accounting for data obsolescence due to natural changes in human biometric features (e.g., aging, injuries), which necessitates periodic database updates and algorithm retraining.

Ethically, the system raises concerns over privacy rights and potential misuse of biometric data, particularly in military contexts. The integration of such systems with autonomous weapons platforms or drones further complicates moral accountability in target identification decisions. Public trust is another critical consideration, as perceived mass surveillance risks eroding confidence in defense institutions.

From a ***legal perspective***, compliance with data protection regulations (e.g., GDPR) and adherence to national/international laws are imperative. Misidentification risks pose serious liabilities, as false positives could lead to wrongful actions with legal repercussions.

Last but not least, operational challenges arise in integrating new technologies with legacy defense infrastructures, requiring seamless compatibility. Comprehensive personnel training is vital to prevent system misuse and operational errors, while the system must also maintain reliability in extreme battlefield conditions—such as poor lighting, high noise levels, and harsh weather—to ensure consistent performance.

4. Conclusions

The implementation of AI-powered biometric recognition systems has transitioned from an opportunity to a necessity for modernizing defense human resource management. By enhancing security, automation, and operational readiness, these systems deliver transformative advantages despite implementation challenges.

Key Advantages - Technology offers enhanced security through robust identity verification, significantly reducing infiltration risks. Simultaneously, it boosts operational efficiency by automating personnel management processes, thereby minimizing administrative burdens. Furthermore, it improves readiness via real-time monitoring and rapid deployment capabilities, ensuring agile responses to dynamic defense needs.

Implementation Framework - Developing such systems requires the integration of advanced technologies, large-scale biometric data collection, and sophisticated algorithm development. The recognition process follows a multi-stage pipeline: data acquisition (collection of raw biometric inputs), preprocessing and feature extraction (noise reduction and pattern isolation), AI model training (adaptive learning for accuracy), verification protocols (real-time validation), and user interface integration (operational deployment).

Critical Balance: Ethics, Law, and Performance - While pursuing technological advancement, strict adherence to three pillars remains non-negotiable: 1) Ethical guidelines, particularly privacy protection, to prevent data misuse; 2) Legal frameworks (e.g., GDPR compliance) to ensure regulatory alignment; 3) Operational standards, guaranteeing reliability in diverse field conditions. This triad ensures public trust while maximizing system efficacy. When properly implemented, AI-biometric systems will revolutionize defense HR management by merging cutting-edge AI with stringent security protocols. Success hinges on navigating technical complexities without compromising ethical principles – a balance that defines the path forward.

Acknowledgements

This work was supported by the NSP SD program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. Д01-74/19.05.2022.

REFERENCES

Alamdari, A., Krovi, V. (2016). A Review of Computational Musculoskeletal Analysis of Human Lower Extremities. In J. Ueda, Y. Kurita (Eds.) *Human Modeling for Bio-Inspired Robotics* (pp. 37 – 73). Academic Press. https://doi.org/10.1016/B978-0-12-803137-7.00003-3.

Grizhebovskaya, A., Mikhalev, A. (2019). Biometric method of human identification based on the vascular pattern of the finger. *Cybersecurity*, *33*(5). 51 – 56.

Prudnik, A. M., Vlasova, G. A., Roshchupkin, Y. V. (2014). *Biometric methods of information protection*. BGUIR.

Patel, U., Gera, K. (2024). Biometric Security Systems Enhanced by AI: Exploring Concerns with AI Advancements in Facial Recognition and Other Biometric Systems have Security Implications and Vulnerabilities. *International Journal of Innovative Science and Research Technology*, *9*(6), 2078 – 2082. https://doi.org/10.38124/ijisrt/IJISRT24JUN1510.

Sokolova A., Konushin, A. (2019). Methods of identifying a person by walking in a video. *Proceedings of the Institute for System Programming of the RAS*, *31*(1), 69 – 82. https://doi.org/10.15514/ISPRAS-2019-31(1)-5.

✉ **Ch. Assist. Prof. Radoslav Chalakov, PhD**
ORCID iD: 0000-0001-6780-9136
Rakovski National Defence College
Command and Staff Faculty
Sofia, Bulgaria
E-mail: r.chalakov@rndc.bg

✉ **Ch. Assist. Prof. Andon Andonov, PhD**
ORCID iD: 0000-0003-1804-483X
Rakovski National Defence College
Command and Staff Faculty
Sofia, Bulgaria
E-mail: a.andonov@rndc.bg

✉ **Assoc. Prof. Viara Jekova, PhD**
ORCID iD: 0009-0007-7037-3653
Rakovski National Defence College
National Security and Defense Faculty
Sofia, Bulgaria
E-mail: v.jekova@rndc.bg