Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.063227

ARTICLE

A Novel Approach to Enhanced Cancelable Multi-Biometrics Personal Identification Based on Incremental Deep Learning

Ali Batouche[1], Souham Meshoul[2,*], Hadil Shaiba[3] and Mohamed Batouche[2,*]

[1]Department of Computer and Information Sciences, Northumbria University, London, E1 7HT, UK
[2]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, 11671, Saudi Arabia
[3]Department of Computer Science, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, 11671, Saudi Arabia

*Corresponding Authors: Souham Meshoul. Email: sbmeshoul@pnu.edu.sa; Mohamed Batouche. Email: mabatouche@pnu.edu.sa

Received: 08 January 2025; Accepted: 04 March 2025; Published: 16 April 2025

ABSTRACT: The field of biometric identification has seen significant advancements over the years, with research focusing on enhancing the accuracy and security of these systems. One of the key developments is the integration of deep learning techniques in biometric systems. However, despite these advancements, certain challenges persist. One of the most significant challenges is scalability over growing complexity. Traditional methods either require maintaining and securing a growing database, introducing serious security challenges, or relying on retraining the entire model when new data is introduced—a process that can be computationally expensive and complex. This challenge underscores the need for more efficient methods to scale securely. To this end, we introduce a novel approach that addresses these challenges by integrating multimodal biometrics, cancelable biometrics, and incremental learning techniques. This work is among the first attempts to seamlessly incorporate deep cancelable biometrics with dynamic architectural updates, applied incrementally to the deep learning model as new users are enrolled, achieving high performance with minimal catastrophic forgetting. By leveraging a One-Dimensional Convolutional Neural Network (1D-CNN) architecture combined with a hybrid incremental learning approach, our system achieves high recognition accuracy, averaging 98.98% over incrementing datasets, while ensuring user privacy through cancelable templates generated via a pre-trained CNN model and random projection. The approach demonstrates remarkable adaptability, utilizing the least intrusive biometric traits like facial features and fingerprints, ensuring not only robust performance but also long-term serviceability.

KEYWORDS: Incremental learning; personal identification; cancelable multi-biometrics; pattern recognition; security; deep learning; cyber-attacks; transfer learning; random projection; catastrophic forgetting

1 Introduction

Biometric recognition systems have gained significant popularity due to their wide range of applications, including access control, identity verification, and forensic investigations. However, as these systems become more prevalent, new challenges arise, such as the need for enhanced security, protection of biometric templates, and adaptability to evolving user characteristics.

Recent research aims to enhance the efficiency of biometric systems while maintaining security and minimizing intrusiveness. The focus has shifted from traditional matching algorithms to deep learning approaches, with an emphasis on improving accuracy and confidence [1,2].

Other concerns about the security of biometric data and the protection of biometric templates have been at the forefront of biometric research. Unauthorized access or disclosure of biometric data can have severe implications for individuals and organizations, prompting the exploration of advanced techniques to safeguard this sensitive information.

Cancelable biometrics has emerged as a solution to address the security and privacy concerns associated with biometric data. Cancellable biometrics are intentionally distorted biometric templates that can be revoked and reissued when required. Numerous studies have proposed different approaches to cancelable biometrics. However, the use of such techniques can sometimes lead to a trade-off with the performance of the proposed biometric system [3]. Furthermore, compliance with recognized standards such as ISO/IEC 24745:2022 can become a challenge in such cases, as this standard emphasizes criteria such as unlikability, revocability, non-reversibility, and performance. Striking a balance between security, efficiency, and scalability becomes imperative, especially when these standards set the benchmark for building secure and privacy-preserving biometric systems.

Most notably, the efficiency and scalability of AI-based solutions in the context of biometric recognition systems have received limited attention in research efforts. Not much work has been conducted in this context. The traditional approach to AI-based biometric recognition often necessitates retraining the entire model when new data becomes available or when system updates are required. This process can easily scale exponentially in complexity in real deployed scenarios, making it cumbersome and computationally expensive [4].

In light of these challenges and the growing importance of efficient and adaptable biometric recognition systems, incremental learning (IL) has emerged as a compelling solution. Incremental learning has the potential to allow biometric systems to learn and adapt incrementally from new data without the necessity of retraining the model from scratch. As such, the system's ability to adapt to changes in user characteristics, variations in biometric traits, and the addition of new individuals to the system can be enhanced using IL.

In this paper, we introduce a novel approach that integrates multimodal biometrics, cancelable biometrics, and incremental learning techniques for biometric identification. This latter is a one-to-many process that uses unique biological traits or characteristics to determine a person's identity amongst others. We focus on identification for numerous reasons. First, identification is more closely aligned with our research's scalability aims. As systems expand and user bases grow, the ability to efficiently identify individuals becomes more important. Second, we emphasize the incremental learning possibilities of biometric systems. Identification processes provide more opportunities for continual development and adaptation, which are critical to our research objectives. Central to the contribution of this work is the development of a 1D-Convolutional Neural Network (1D-CNN) model designed for incremental scalability, in the sense that it can efficiently expand and adapt its architecture as the user base grows without the need for full model retraining. This model serves as a key component within the proposed cancelable multimodal system, enhancing security and efficiency. By combining face and fingerprint traits and adapting to evolving user bases, our method offers significant improvements in the accuracy and robustness of the used datasets.

Therefore, the contributions of this work can be summarized as follows:

- A unified incremental and scalable approach: this work is among the first attempts to integrate incremental deep architectural updates with continuous secure template generation without exhaustive retraining.
- A comprehensive experimental study that investigates the incremental learning capabilities of the proposed approach, including three scenarios based on data-splitting strategies to simulate incrementality and the use of various performance metrics and various variants for comparison purposes.

- High performance with least-intrusive biometrics: The proposed system achieves accuracy rates ranging from 98.33% to 99.68%, with minimal catastrophic forgetting when using facial features and fingerprints.

The remainder of this paper unfolds as follows. In Section 2, we present the key topics addressed in this work emphasizing the significance of multimodal biometrics, cancelable biometrics, and incremental learning within the domain of biometric recognition systems. Section 3 is devoted to a comprehensive review of related literature while identifying some research gaps. Section 4 delves into the methodology and technical inner workings of the proposed approach. Section 5 offers insights into our experimental setup, encompassing datasets, performance metrics, and evaluation results. Finally, Section 6 provides a conclusive summary of our contributions and outlines promising avenues for future research.

2 Background

Biometric systems have played a pivotal role in security and identification processes for several decades. These systems utilize unique biological or behavioral traits for authentication and identification, offering a more secure alternative to traditional methods such as passwords and ID cards. Biometric traits encompass a wide range of body measurements and characteristics associated with individuals. These include physiological traits such as fingerprints, facial features, and iris patterns, as well as behavioral traits like voice, gait, and signature. Each type of biometric trait offers distinct advantages and challenges in terms of accuracy, ease of collection, user acceptance, and susceptibility to forgery. A deeper exploration of biometrics systems can be found in [5]. This research encompasses two primary domains: cancelable multimodal biometrics, and incremental learning. Before delving into the proposed methodology, we first provide a concise overview of these areas to ensure clarity and comprehensiveness within the paper content.

2.1 Cancelable and Multimodal Biometrics

Biometric systems face significant challenges, particularly around the security and privacy of biometric data. Unlike passwords, biometric traits cannot be changed if compromised. As highlighted in [3], stolen biometric data can lead to spoofing attacks, where counterfeit traits are used to gain unauthorized access. This poses a major risk to the integrity of biometric systems.

Given the security challenges associated with traditional biometric systems, it is essential to ensure the protection and confidentiality of biometric templates. Cancelable biometrics addresses this concern by transforming original biometric data into a cancelable form. This concept, first introduced in [6], refers to the technique used to mitigate the risks associated with the long-term storage of biometric traits. It differs from traditional biometric systems in that it transforms raw biometric data into a unique, revocable template.

A cancelable biometric template is built upon four fundamental principles:

- Diversity: To ensure security, each application requires a distinct template.
- Reusability/Revocability: For enhanced privacy, compromised templates can be revoked and replaced with new ones.
- Non-invertibility: To safeguard sensitive biometric data, the original information cannot be recovered from the template.
- Performance: The transformation process must preserve the system's ability to accurately recognize individuals.

Various methods for generating cancelable biometric templates have been proposed, each with its advantages and disadvantages. Template generation methods can be broadly categorized into six types [3]: cryptography-based, transformation-based, filter-based, hybrid, or multimodal methods. Each approach offers distinct trade-offs between security and efficiency. Cryptography-based methods prioritize strong

security but often require significant computational resources. Transformation and filter-based methods emphasize efficiency but may have limitations in terms of security. Hybrid methods aim to balance both security and efficiency, while multimodal methods leverage multiple biometric traits for enhanced security but may be constrained by data availability.

Multimodal biometric recognition systems suggest combining multiple biometric traits, such as face, fingerprint, iris, or voice to benefit from the complementary strengths of each modality. This fusion of different biometric characteristics helps improve recognition performance, reduce error rates, and enhance system security and robustness. A review of multimodal biometrics systems can be found in [3]. Several combinations of biometric traits have been investigated such as in [7,8].

2.2 Incremental Learning

Incremental learning, also known as continual or lifelong learning, is a machine learning approach that allows models to continuously learn from a stream of incoming data without requiring retraining from scratch. Unlike traditional batch learning, which processes data in large, static datasets, incremental learning enables models to update and adapt as new information becomes available. This is particularly suitable for dynamic environments where data is constantly evolving.

Various strategies and mechanisms have been used to achieve IL as suggested by Wang et al. in [9]. While regularization-based methods impose constraints to limit model changes and preserve past knowledge, replay-based strategies also known as rehearsal-based strategies, reintroduce past experiences during new training, either by storing previous data (experience replay) or generating synthetic data (generative replay). Another category encompasses optimization-based techniques that modify the training process to ensure new tasks don't interfere with previous ones. On their side, architecture-based approaches adjust the model's structure by adding new layers or modules to handle new tasks while retaining old functionality. Finally, hybrid approaches combine elements from multiple methods, balancing the strengths of each to improve performance. While these categories provide distinct strategies, many techniques overlap and share common principles in their efforts to balance new learning with knowledge retention.

In terms of assessment, two key metrics are often used to evaluate the effectiveness of incremental learning frameworks: Backward Transfer (BT) and Forward Transfer (FT). These metrics assess how learning new tasks influences the model's performance on both previously learned and future tasks [10–12].

Particularly, BT describes how learning a new task can impact the performance of previously learned tasks. Positive BT occurs when learning a new task enhances performance on older tasks. Conversely, negative BT, also known as catastrophic forgetting, when significant, happens when learning a new task negatively affects the performance of previously learned tasks [12].

3 Related Works

3.1 Overview of Existing Approaches

Biometric recognition systems have evolved from traditional methods based on hand-crafted features to deep learning models. Numerous studies, including [13], have validated the efficacy of deep learning models for biometric recognition. Similarly, the power of multimodal biometrics has been substantiated by a wealth of research, as exemplified by [14] and [15]. On another side, cancelable biometrics emerged as a response to the growing need for stronger template protection. The authors of [16] proposed a biometric template security method that involves symmetric-key encryption and Bloom filter transformation, preserving data format and recognition accuracy.

Template generation must remain computationally efficient as system complexity increases. The ISO/IEC 24745:2022 standard outlines the protection requirements for biometric information, emphasizing confidentiality, integrity, and renewability during storage and transfer. It also mandates that security measures, such as Biometric Template Protection (BTP) techniques, do not significantly degrade system performance [17]. Random projections, as demonstrated in [18], offer a computationally efficient dimensionality reduction technique that effectively preserves data structure, making them suitable for practical biometric systems, especially when compared to traditional methods like PCA and LDA.

Scalability remains a critical issue in biometric systems, particularly as datasets grow larger. Incremental learning and transfer learning address this by allowing models to adapt without fully retraining from scratch. For example, authors in [19] developed an incremental support vector machine (SVM) model that updates using new ECG data without losing previously learned information. This method significantly reduced the false acceptance rate from 6.49% to 4.39%, but its reliance on traditional SVMs may limit scalability in larger datasets compared to neural networks. On the other hand, the study described in [20] used a multitask learning approach integrating face and fingerprint recognition, achieving over 80% accuracy using incremental LDA. This approach demonstrated better scalability and adaptability for real-time identification, especially in systems requiring continuous updates.

Authors of [21] introduced a cancellable biometric authentication framework that uses phase-wise incremental learning to adapt to new enrollments without full retraining. The framework secures CNN-generated biometric templates with SHA-3 hashes and employs a KNN classifier to expand the decision pool dynamically. The framework is evaluated on multiple iris and knuckle-print datasets, achieving an almost perfect correct recognition rate with low to varying EER depending on the constraints of the scenario. On another side, spoof fingerprint detection was addressed in [22] where the authors addressed the stability-plasticity dilemma. The model integrates ResNet-50 for extracting deep features and an ensemble of base SVM classifiers and employs a few-shot learning strategy for incremental updates. The model demonstrated significant performance gains on new spoof materials with an average accuracy improvement of 49.57% between consecutive learning phases. In the same context of fingerprint identification, a distributed system that uses a hierarchical classification approach was introduced in [23] to improve efficiency. By combining multiple feature extractors and employing a strategic search process, the system achieved high accuracy while significantly reducing the number of database comparisons. The authors demonstrated the system's effectiveness and its high accuracy rates for both segmented (93%) and non-segmented (91%) fingerprints, as well as its ability to minimize database penetration.

An Incremental Granular Relevance Vector Machine (iGRVM) for multimodal biometric score classification was proposed in [24]. The iGRVM has been found as an efficient model that can update its decision boundary as new data becomes available. It achieved comparable accuracy (94.12%) to traditional methods while significantly reducing training time.

The study in [25] proposed an incremental learning approach for gait recognition that handles varying viewpoints and walking conditions. By using a CNN and memory-based strategy, the model effectively integrates new data without forgetting old information. The results showed that the approach outperforms traditional methods, especially for large and unbalanced datasets. In the area of EEG biometric recognition, a system was proposed in [26] where the authors propose an incremental EEG biometric recognition system that uses an EEG Relation Network for short-time resting-state signals. This model achieved high accuracy rates, ranging from 86.7% to 93.3%, by using a few-shot learning strategy to adapt to new data. In a different context, authors in [27] propose an incrementally designed secure biometric identification system built on an existing legacy system. The approach updates the legacy system's codebook and user enrollments to

enhance identification rates and secret key generation using helper data and a noisy memoryless channel while minimizing privacy leakage.

In [28], authors propose GBDTNN, an incremental learning-based authentication model that integrates Gradient Boosting Decision Tree (GBDT) for processing high-dimensional features and a Neural Network for online updates. The purpose of such a combination is to allow the system to adapt to changes in user behavior, making it more secure and user-friendly. They achieved about 95.96% accuracy, with an equal error rate of 4.01%, a false acceptance rate of 4.88%, and a false rejection rate of 3.03%. In the area of face recognition, an incremental learning approach for open-set video face recognition using low-labeled stream data is proposed in [29]. The model combines a deep features encoder with Open-Set Dynamic Ensembles of SVM to identify individuals of interest. The system can adapt to new patterns and avoid catastrophic forgetting, leading to a significant improvement in performance. The proposed method shows a benefit of up to 15% F1-score increase compared to non-adaptive state-of-the-art methods.

3.2 Critical Analysis

To further analyze and compare these approaches, Table 1 provides a detailed comparison of the key aspects of most related approaches. A significant portion of early research on incremental biometric systems primarily focused on deployment-related frameworks rather than learning methodologies. These studies explored incremental approaches for updating legacy systems or managing data storage to handle newly enrolled users efficiently. While these methods addressed operational challenges, such as scalability in deployment, they did not tackle the complexities of incremental learning itself—particularly in adapting models to accommodate new classes or data without requiring full retraining. Furthermore, a significant portion of current research relies on machine learning techniques, such as KNN and SVM ensembles, which inherently support incremental updates. As the number of users grows, the complexity of these models increases significantly, making them impractical for dynamic, real-world scenarios.

Table 1: Comparative analysis of incremental learning approaches in biometric systems (FE: Feature Extraction, CL: Classifier, CT: Cancelable Template)

Ref.	Models	Datasets	Cancelable biometrics	Multimodal biometrics	Class incremental learning	Architectural changes	Handling catastrophic forgetting
[21]	FE: CNN CL: KNN	PolyU-FKP, IIT Delhi-V1, UBIRIS-V2, CASIA datasets	Yes	"Trait Agnostic"	Yes	No	Observed through EER percentages
[22]	FE: ResNet-50, CL: ensemble of SVMs	LivDet datasets	No	No	–	Yes	Assumes RBF SVM are free from catastrophic forgetting
[23]	FE: Multiple FEs, CL: Random Forest and SVMs	NIST: SD4, SD14, and SFinGe	No	No	Yes	Yes	Not explicitly calculated

(Continued)

Table 1 (continued)

Ref.	Models	Datasets	Cancelable biometrics	Multimodal biometrics	Class incremental learning	Architectural changes	Handling catastrophic forgetting
[24]	Relevance Vector Machine (RVM), Granular and incremental	CASIA-IRIS-Distance v4, BioSecure DS2, BSSR1	No	Yes	Yes	No	Not explicitly calculated
[25]	CNN	CASIA-B	No	No	No	No	Inferred from accuracy results
[26]	EEG Relation Network (EEG-RN)	Physionet EEG Motor Move-ment/Imagery Dataset	No	No	Yes	No	Not explicitly calculated
[28]	Gradient Boosting Decision Tree (GBDT), Neural Network (NN)	Custom smartphone data	No	No	No	No	Not explicitly calculated
[29]	Deep features encoder, Ensembles of SVM (OSDe-SVM)	CMU, COX, YouTube Faces Dataset	No	No	Yes	Yes	Assumes ensemble methods overcome catastrophic forgetting
Our Proposed approach	CT: ResNet-50 and Random Projection, CL: Dynamic 1D-CNN	[30,31]	Yes	Yes	Yes	Yes	Inferred from accuracy on incremental cumulative sets

Similarly, some methodologies focus on incrementally refining existing data representations with continuous data integrations. While this improves and maintains classification quality over time, it does not address the key challenge of class-incremental learning, where new user classes must be integrated without triggering a full retraining process. In such cases, the model must reprocess all prior data to preserve its performance. Moreover, many approaches neglect the integration of robust template security mechanisms, leaving gaps in their ability to safeguard biometric data against attack vectors such as data poisoning or impersonation. Dynamic architectural updates, which are critical for adapting model structures to accommodate new classes efficiently, are also rarely implemented. Additionally, while some studies address catastrophic forgetting, most either assume that ensemble models are inherently resistant to it or infer their capabilities based on overall performance metrics without explicitly measuring it.

Overall, the findings presented in these studies underscore the potential of incremental learning to address scalability and adaptability challenges in biometric systems.

4 Proposed Incremental Deep Learning Approach

Given the identified challenges and gaps in the literature, this study aims to achieve the following research goals:

- Expand upon recent advances in biometric systems to incorporate robust and scalable solutions.
- Formulate a comprehensive model that seamlessly integrates cancelable biometrics (to enhance security), scalability via dynamic architectural updates, and advanced deep learning techniques to optimize performance while effectively managing the trade-offs among these critical components within a unified framework.

To this end, we propose a novel approach to personal identification, as illustrated in Fig. 1. The figure outlines the main stages of our proposed approach, illustrating both the enrollment and identification (or recognition of enrolled individuals) processes.

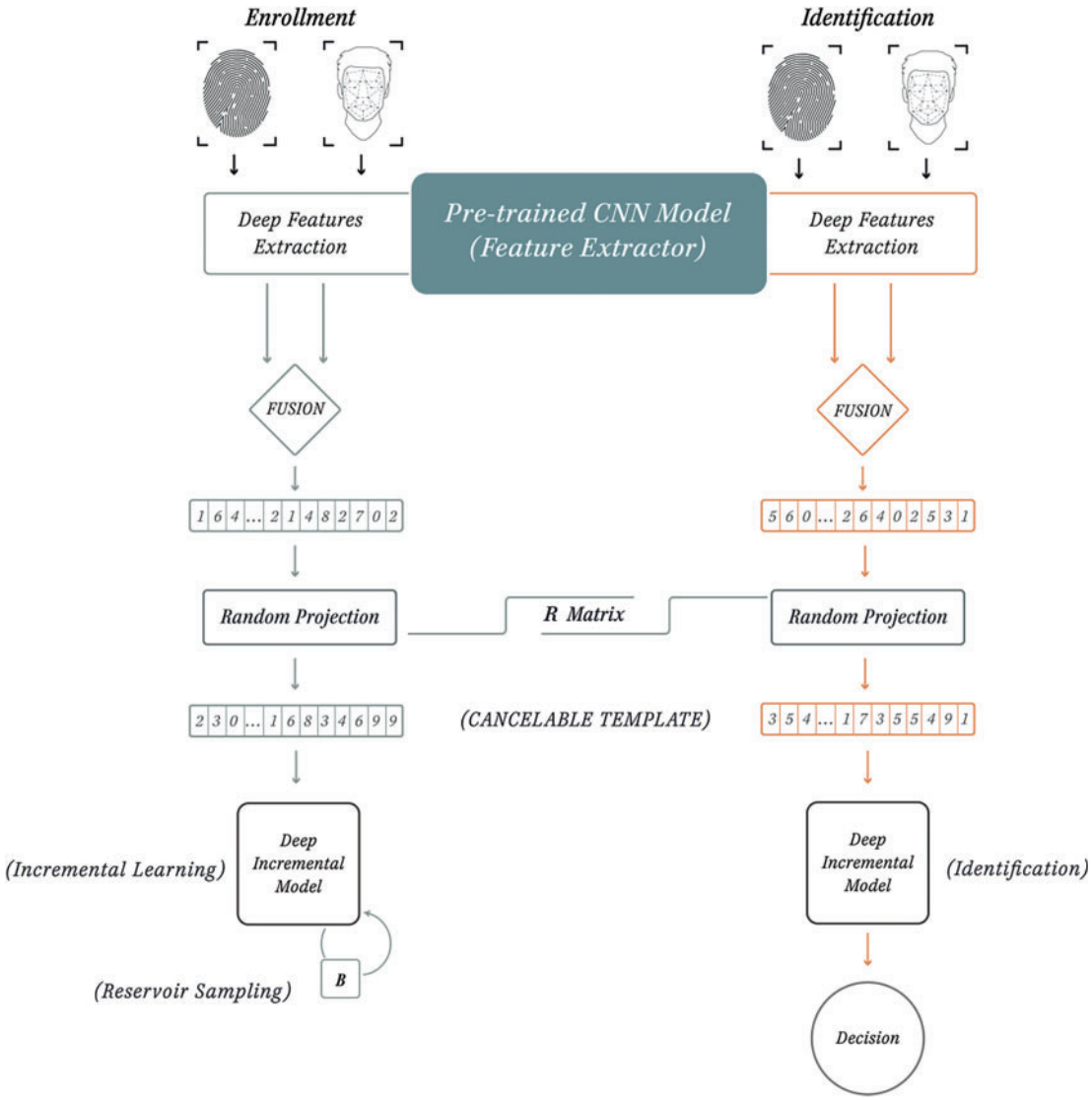

Figure 1: Overview of the proposed system, illustrating the enrollment (Left) and identification (Right) phases

During enrollment, biometric inputs are processed through a pre-trained CNN for feature extraction, followed by feature fusion and random projection to generate cancelable templates. Reservoir sampling is applied to the buffer (B), and the model is incrementally trained on new data. In the identification phase, the incremental model leverages the generated templates for identity verification, ensuring efficient and secure decision-making.

At the core of our system is an incremental deep learning model based on CNN, which continuously adapts as new individuals are enrolled. We simulate this process using an incremental dataset, where new users are introduced over time. The system's learning process is dynamic, allowing it to update its knowledge without requiring retraining from scratch. Identification benchmarks are conducted using test sets. Another key aspect of our system is the use of cancelable biometrics to ensure the security of collected biometrics. By employing deep feature extraction and random projection, we aim to strike a balance between security (through increased complexity) and system performance. This ensures that sensitive biometric data remains protected without compromising recognition efficiency.

4.1 Selection of Biometric Identifiers and Data Preparation

The choice of biometric identifiers is critical, as it directly affects the system's usability and effectiveness. Intrusive biometric methods like iris scans and vein patterns, though highly accurate, often face challenges related to user discomfort and practical limitations in real-world applications, as has been explored in research such as [32,33]. On the other hand, several other studies confirm that multimodal biometrics, which combines traits like face, fingerprint, and iris, provide better reliability and security by reducing vulnerability to spoofing attacks and improving accuracy [3].

Since our goal is to scale efficiently and seamlessly, ensuring user convenience is critical. Hence, we have selected face and fingerprint scans as the biometric traits for our system. These identifiers, although considered hard biometrics, are relatively less intrusive while offering strong performance in biometric systems, as observed in [14,20].

Facial features are naturally strong identifiers for individuals. Moreover, a person's face is usually visible and globally accessible, making facial recognition feel less intrusive compared to methods like iris scans. However, relying solely on facial features can expose the system to vulnerabilities such as spoofing attacks, and raising privacy concerns. To mitigate these risks, we combine facial recognition with the more robust and widely studied fingerprint scans. Fingerprint scans provide excellent performance without requiring advanced tools, and users are generally more accepting of sharing this trait. In fact, most modern smartphones use fingerprint scans for unlocking devices, making people more comfortable and familiar with this form of identification. This makes fingerprint scans particularly suitable for real-world applications. We built our dataset by merging two datasets sourced from Kaggle [30,31]: a face recognition dataset containing images of individuals captured from various angles, with diverse expressions, hairstyles, and occlusions, and a fingerprint dataset consisting of multiple scans per individual. The combined dataset was then preprocessed to include data from thirty-one individuals, with each individual having thirty face and fingerprint scans. This dataset forms the foundation for our subsequent experiments.

Since our study explores the scalability aspect of biometric systems through incremental learning, we truncated the dataset into several increments to investigate several evaluation scenarios, as can be seen in Fig. 2. Below is an overview of the datasets generated for different purposes:

- Incremental Sets: This subset is specifically designed for the incremental learning scenario. Each increment represents the introduction of a new individual into the system, simulating a real-world scenario where individuals are enrolled over time. In each increment, we introduce a new individual's

biometric identifiers for both training and testing. The model is trained and tested on individual increments to evaluate its performance in recognizing new individuals. Let's denote the overall dataset as D, which contains biometric samples for N individuals:

$$[D = \{(x_1, y_1), (x_2, y_2), \ldots, (x_N, y_N)\}] \tag{1}$$

where x_i represents the biometric identifier (features) and y_i is the corresponding label (identity of the individual).

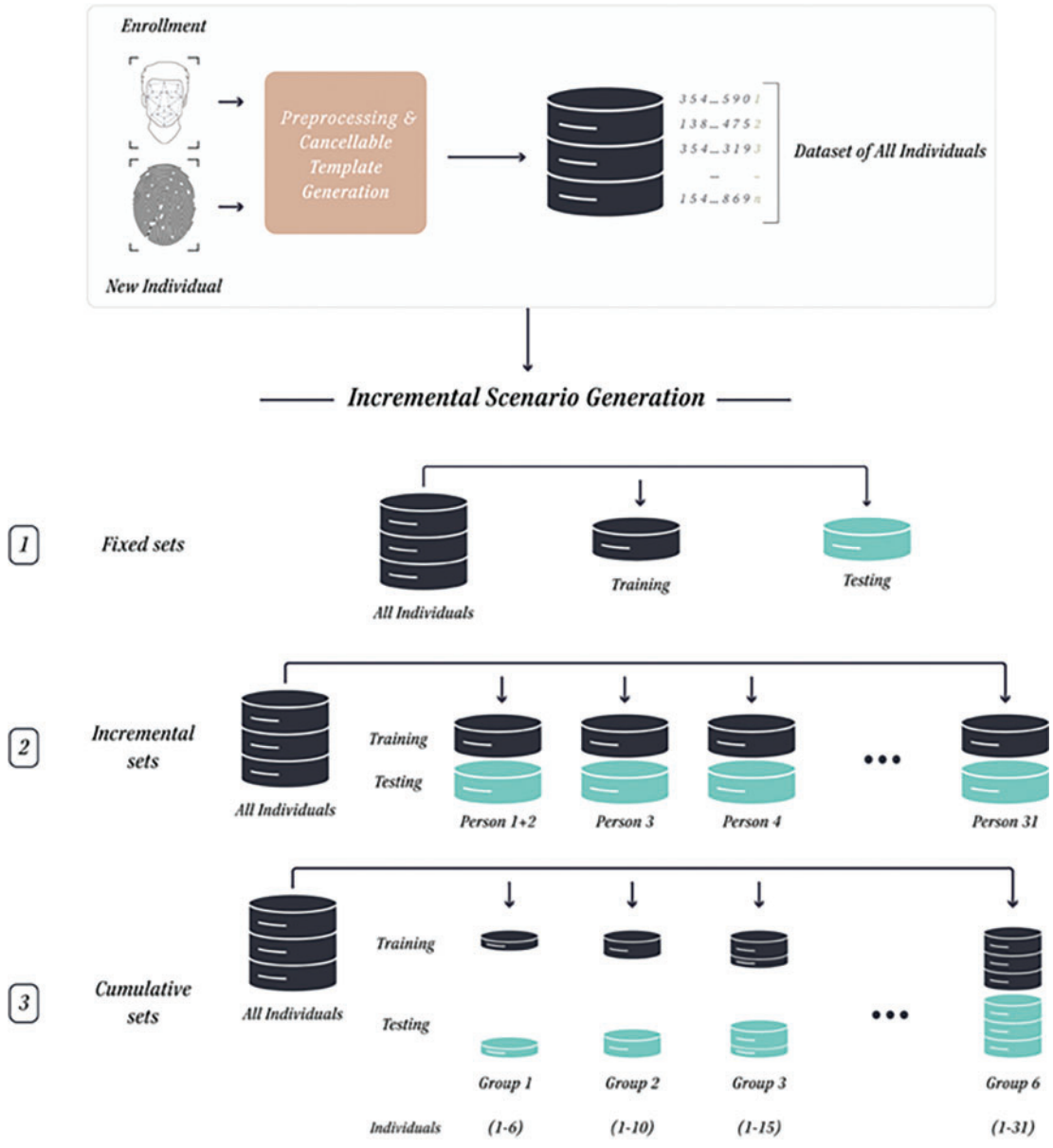

Figure 2: Data preparation steps and incremental scenarios generation. All biometric samples are collected and preprocessed into a comprehensive dataset of cancelable templates. From this dataset, three evaluation scenarios are generated: (1) A fixed dataset, (2) Granular increments, and (3) Cumulative increments, each with distinct training and testing splits

The dataset is then partitioned into T increments, each containing the biometric data of m_t individuals:

$$D = \bigcup_{t=1}^{T} D_t \quad \text{where} \quad D_t = \{(x_{i_t}, y_{i_t})\} \; and \; |D_t| = m_t \tag{2}$$

D_t: The subset of data introduced in the tth increment.

m_t: The number of individuals introduced in the tth increment.

In this scenario, at each increment t, the model is trained on the current increment subset D_t and tested on the same increment:

$$\text{Train}\left(M_t, D_{t(train)}\right) \quad \text{Test}\left(M_t, D_{t(test)}\right)$$

where M_t is the model after training on increment D_t. The evaluation at each increment tests the model's ability to recognize new individuals introduced in D_t.

- Cumulative Sets: We also prepare a set of cumulative datasets for training and testing. In the cumulative sets' scenario, after each new increment, the dataset grows to include data from all previous increments. This setup allows us to evaluate how well the model retains knowledge of previous individuals and handles BT. Let's define the cumulative dataset at increment t as:

$$D^t_{\text{cumulative}} = \bigcup_{k=1}^{t} D_k \tag{3}$$

At each step, the model is trained on the entire cumulative dataset $D^t_{\text{cumulative}}$, which includes data from all prior increments:

$$\text{Train}\left(M^t_{\text{cumulative}}, D^t_{\text{cumulative(train)}}\right) \quad \text{Test}\left(M^t_{\text{cumulative}}, D^t_{\text{cumulative(test)}}\right)$$

This tests the model's ability to recognize both old and new individuals over time, and BT can be evaluated by comparing the model's performance to earlier increments as more increments are added.

- Fixed Training and Testing Sets: In this scenario, we use a fixed portion of the dataset that includes biometric identifiers of all individuals for both training and testing. This serves as a benchmark to measure the upper-bound performance of the model when it has access to the full dataset from the beginning. The fixed dataset is denoted as:

$$D_{\text{Fixed}} = D \tag{4}$$

The model is trained on the entire dataset and then evaluated to provide a comparison point with the incremental learning models:

$$\text{Train}\left(M_{\text{Fixed}}, D_{\text{Fixed(train)}}\right) \quad \text{Test}\left(M_{\text{Fixed}}, D_{\text{Fixed(test)}}\right)$$

This allows us to benchmark the incremental model's performance (over time) against an optimized model that has full access to all the data.

4.2 Cancelable Template Generation

Various methods for generating cancelable biometric templates have been proposed, each with its advantages and disadvantages. A comprehensive survey on cancelable biometrics can be found in [3] where

a taxonomy of cancelable biometric template generation methods is provided. According to the proposed taxonomy, broadly the methods can fall into one of six categories namely Cryptography-based methods, Transformation-based methods, Filter-based methods, Hybrid methods, and Multimodal methods. Each of these methods has its advantages and disadvantages. For instance, Cryptography-based methods provide strong security but may be computationally expensive. Transformation-based methods can provide good performance but may be susceptible to certain types of attacks. Filter-based methods can be efficient but may not offer the same level of security as cryptography-based methods. Hybrid methods can provide strong security and good performance but may be complex to implement. Multimodal methods can provide strong security and good performance but require multiple biometric traits, which may not always be available.

Random projections, on the other hand, offer a good balance between security and computational efficiency, as seen in [34]. The authors provided empirical evidence showing that random projections effectively preserve cosine and subspace structures, making them suitable for practical biometric systems. Compared to traditional dimensionality reduction techniques like PCA and LDA, random projections offered a more computationally efficient alternative while still preserving critical data characteristics.

In our study, cancelable template generation is a two-stage process. First, we leverage the power of deep learning techniques and transfer learning, specifically CNNs as feature extractors, to get discriminative and high-level features from the selected biometric identifiers called deep features. A plethora of pre-trained CNN models are available for this purpose. Our approach involves employing the ResNet-50 model to extract deep features from facial and fingerprint data. For each identifier, a 2048-dimensional feature vector is extracted and then concatenated to form a 4096-dimensional combined feature vector:

$$df\text{combined} = \left[df_{\text{face}}; df_{\text{fingerprint}}\right] \in R^{4096} \tag{5}$$

Afterward, a random projection is used to generate the cancelable template:

$$T\text{cancelable} = R * df\text{combined} \tag{6}$$

where R is a random matrix and * denotes the matrix multiplication.

To perform the random projection, a random matrix R is employed, with the entries of the matrix drawn from a Gaussian distribution. Its foundation is the Johnson-Linden Strauss lemma [35], which states that high-dimensional data can be projected into a lower-dimensional space with minimal distortion of the distances between points. This procedure will ensure that the original data's structure is preserved, thereby simplifying its handling and processing steps while ensuring compliance:

1. Non-Invertibility: By projecting data into a lower-dimensional space, random projection can be employed to anonymize it, thereby preventing the identification of individual data points. Thus, the transformation is a one-way function, ensuring that the original biometric data and dfcombined cannot be reconstructed from Tcancelable.
2. Diversity: The number of random matrices that can be generated is theoretically infinite. This is because the random matrix is composed of elements that are typically selected from a continuous probability distribution. Therefore, there are infinitely many possible combinations of values for the elements of the matrix.
3. Revocability: If a template is compromised, a new cancelable template can be issued by applying a different random transformation R, generating a new template $T^{new}_{Cancelable}$.
4. Performance Preservation: The random matrix is generated in such a way that it approximately preserves the pairwise distances between points in the original high-dimensional space. Thereby, the random

projection maintains the discriminative properties of the original data, ensuring separability between different individuals and preserving recognition performance.

Therefore, the main reasons that explain the use of random projection in our work are that random projection is a computationally efficient and scalable method for biometric template protection, offering benefits such as ease of revocation and re-issuance through modification of the random projection matrix, inherent privacy preservation by transforming biometric data into a non-invertible format, and a proven track record of achieving good accuracy and security in a variety of scenarios. Furthermore, while the dimensionality of the data is reduced, the discriminative properties are retained.

4.2.1 Security Analysis of the Cancelable Template Generation Process

Random projection reduces the dimensionality of biometric data, mapping it into a lower-dimensional space while introducing information loss that complicates the reconstruction of the original data. This inherent property offers a significant degree of protection against inversion attacks, ensuring that even if the transformed data is exposed, the original biometric information remains secure. The random matrix utilized in the projection can be generated in numerous ways, enabling the creation of unique transformations tailored to specific applications. In the event of a compromised biometric template, the system can revoke and reissue a new template by applying a distinct random projection matrix, thereby facilitating template revocation and re-issuance. This capability enhances the security and adaptability of the biometric system.

The security of random projection is contingent upon its implementation and the specific threat model under consideration. If the random projection matrix is not stored or is discarded after application, it becomes computationally infeasible to reverse-engineer the original biometric data, even in the event of a compromised transformed template. While random projection significantly enhances security, it is not immune to all forms of attacks and can be, as a transformation-based method, vulnerable to some attacks such as correlation attacks. Consequently, it is advisable to integrate random projection with additional security mechanisms. For this purpose, we combined random projection with deep feature extraction using pre-trained convolutional neural networks (CNNs). Deep features derived from CNNs are generally regarded as non-invertible, meaning that accurately reconstructing the original input data from these features is highly challenging. This is due to the complex and non-linear transformations applied by convolutional layers, activation functions, and pooling layers, which collectively make the inversion process to recover the original biometric data exceedingly difficult.

Additionally, since we are utilizing multimodal biometric data (both facial and fingerprint identifiers), the system offers enhanced security. The use of multiple biometric identifiers makes it significantly harder to compromise or hack the system, as an attacker would need to breach multiple modalities simultaneously, further securing the biometric templates.

The security of our random projection-based template protection scheme relies on the inherent difficulty of reconstructing the original deep feature vector, x, from the projected template, y, without knowledge of the random projection matrix, R as described in Eq. (6) where y refers to the cancellable template of reduced dimensionality, (Tcancelable), and x refers to the original high-dimensional deep feature vector (dfcombined). Since random projection reduces the dimensionality of the data, the number of unknowns (the dimensions of x) exceeds the number of equations (the dimensions of y). Therefore, the system to be solved for x given y is underdetermined which means there exists an infinite number of potential solutions for x. Hence, an attacker attempting to invert this projection faces the challenge of solving an underdetermined system of linear equations, particularly in the absence of prior knowledge of R. The computational complexity of finding one such solution is generally $O(n^3)$ using standard matrix inversion techniques, where n is the

dimensionality of the original deep feature vector x. Moreover, simply finding a solution does not equate to breaking the system, as the attacker needs to find the correct original feature vector.

4.3 Proposed Incremental Deep Learning Model

The primary components of our model include a 1D-CNN including a convolutional block and an incremental MLP classifier (fully connected layers). Fig. 3 outlines the structure of our proposed model and full implementation with results can be found in [36].

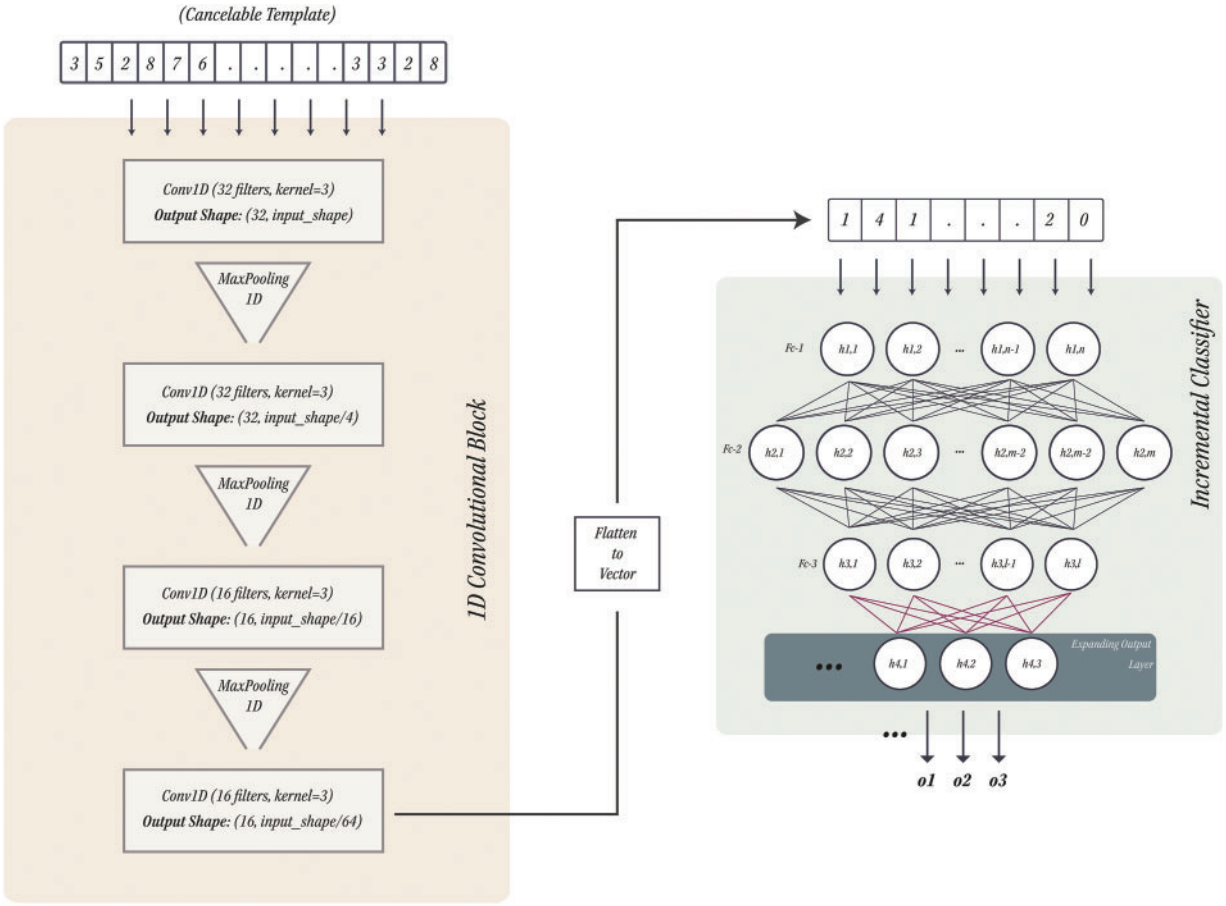

Figure 3: Proposed model 1D-CNN architecture with dynamically expanding output layer. (Left) 1D convolutional layers, (Right) Fully connected layers (Incremental Classifier)

Cancellable biometric templates derived from facial features or other biometric traits, often exhibit a structured, sequential format. A 1D-CNN is particularly well-suited to this type of data due to its ability to efficiently capture local patterns. This makes it ideal for processing biometric sequences or vectors that reflect these structured patterns.

Our proposed model consists of an incremental 1D-CNN that receives cancellable templates as input. It is designed to continually expand and adapt as new individuals are enrolled. The 1D-CNN convolutional block is composed of four convolutional layers, each followed by max-pooling operations to capture the temporal and spatial dependencies within the cancellable biometric template data.

The network progressively reduces the feature space to a manageable form before passing it to the incremental classifier block. Each convolutional layer applies the following operation:

$$y^{(l)} = \sigma\left(x^{(l)} * g^{(l)}\right) \tag{7}$$

where:

- $x^{(l)}$ is the input to the lth convolution layer,
- $g^{(l)}$ is a kernel for the convolutional layer,
- $*$ denotes the convolution operation,
- σ is the ReLU activation function,
- $y^{(l)}$ is the output after the ReLU activation function.

The MaxPooling layer applies a down-sampling operation over each feature map to reduce its spatial dimensions:

$$y^{(l)} = \text{maxpool}\left(x^{(l)}\right) \tag{8}$$

The incremental classifier is designed to dynamically adapt as new users are enrolled. This is accomplished through an adaptation method that expands the classifier as new biometric identities are introduced. Rather than requiring full model retraining, the classifier efficiently integrates these new classes by expanding its output layer incrementally.

Table 2 provides a detailed description of the functions and input-output of each layer and parameters in the proposed model architecture shown in Fig. 3.

Table 2: Summary of model layers and parameters

Layer (Type: Depth-Idx)	Input shape	Output shape	Param #
Conv1d: 1–1	[−1, 1, 4096]	[−1, 32, 4096]	128
MaxPool1d: 1–2	[−1, 32, 4096]	[−1, 32, 1024]	–
Conv1d: 1–3	[−1, 32, 1024]	[−1, 32, 1024]	3104
MaxPool1d: 1–4	[−1, 32, 1024]	[−1, 32, 256]	–
Conv1d: 1–5	[−1, 32, 256]	[−1, 16, 256]	1552
MaxPool1d: 1–6	[−1, 16, 256]	[−1, 16, 64]	–
Conv1d: 1–7	[−1, 16, 64]	[−1, 16, 64]	784
MaxPool1d: 1–8	[−1, 16, 64]	[−1, 16, 16]	–
Linear: 1–9	[−1, 256]	[−1, 300]	77,100
Linear: 1–10	[−1, 300]	[−1, 128]	38,528
Linear: 1–11	[−1, 128]	[−1, 2] *(initially)*	258
Estimated total size (MB)		1.77	

Drawing inspiration from implementation principles in [37,38], the incremental adaptation process is outlined in the following process. Moreover, to maintain performance in previously learned classes, the training process incorporates Elastic Weight Consolidation (EWC) and a rehearsal buffer.

Incremental_learning (input, experience, rehearsal_buffer):

 # Step 1: Adaptation Phase

1.1 Detect new classes from the experience

1.2 If new classes are detected:

1.2.1 Preserve weights and biases for previously learned classes

1.2.2 Expand the classifier output layer to accommodate new classes

 # Step 2: Training Phase

2.1 Prepare training data by combining (current_experience_data, rehearsal_buffer)

2.2 Train 1D-CNN using (Cross-Entropy Loss, EWC regularization)

 # Step 3: Identification Phase

3.1 Pass input through the model

3.2 Compute predictions directly using the classifier's output

3.3 Return predictions for all active classes

EWC penalizes updates of important parameters based on their significance to previously learned classes, preserving the weights of old units and reducing the impact of new classes on previously learned classes. Accordingly, the loss is calculated as follows [39]:

$$\mathcal{L}(\theta) = \mathcal{L}_{new}(\theta) + \sum_i \frac{\lambda}{2} F_i (\theta_i - \theta_i^*)^2 \tag{9}$$

where:

- $L_{\text{new}}(\theta)$ is the loss for the new task.
- θ_i represents the parameters of the model.
- θ_i^* are the optimal parameters from previous tasks.
- F_i is the Fisher Information matrix.
- λ is a regularization hyperparameter that controls the balance between new learning and old knowledge retention.

On the other hand, the rehearsal buffer applies a reservoir sampling strategy, randomly selecting a subset of previous samples (up to 1000 samples initially) to be included in the training process alongside new samples. This allows the model to learn from a mixture of old and new samples during incremental training. We denote the buffer update function as follows:

When a new sample (x_t) is introduced, it is incorporated into the buffer based on the following probability:

$$P(\text{replace}) = \frac{K}{t} \tag{10}$$

where K is the size of the buffer and t is the total number of samples seen so far.

The probability (Eq. (10)) determines whether the new data D_t should replace an existing item in the buffer. The buffer is updated based on the following rule:

$$Buffer\_Update(B, D_t) = \begin{cases} B \cup D_t & if |B| + |D_t| \leq \text{buffer}_{\text{limit}} \\ Replace\ a\ random\ element\ in\ B, & if |B| + |D_t| > \text{buffer\_limit with probability P (Replace)} \end{cases}$$

While reservoir sampling introduces a level of randomness in selecting a subset of previous samples, it is specifically designed to maintain a representative distribution of past data, ensuring that the model does not develop a bias toward either older or newer data. This method allows the model to generalize effectively while mitigating the risk of performance degradation on specific sample groups [40].

4.4 Evaluation Scenarios and Metrics

To evaluate the performance of the model, various scenarios and metrics have been considered according to the scenarios for data generation shown in Fig. 2. Let us denote by $f(M, D)$ a generic function representing the performance metric value (accuracy, precision, recall, F1-score, ...) of model M on an increment D.

First, the model's incremental learning performance at each increment number t is measured by evaluating the performance metrics on the current increment D_t. This is represented as:

$$\text{Performance}^{t}_{\text{incremental}} = f(M_t, D_t) \tag{11}$$

Next, we assess the cumulative performance, which reflects how well the model retains knowledge of previously learned individuals while continuing to learn new individuals. The cumulative performance is evaluated on the dataset that includes all previous increments up to D_t:

$$Performance^{t}_{cumulative} = f\left(M^{t}_{cumulative}, D^{t}_{cumulative}\right) \tag{12}$$

Additionally, we assess BT, which evaluates the model's ability to retain and improve on previously learned tasks. BT is measured by calculating the change in performance on earlier increments after learning new increments:

$$B_t = \frac{1}{t-1}\sum_{k=1}^{t-1}\left(f\left(M^{t}_{\text{cumulative}}, D_k\right) - f\left(M^{t-1}_{\text{cumulative}}, D_k\right)\right) \tag{13}$$

Finally, the fixed benchmark performance is the model's best achievable performance using the entire dataset D, providing a comparison point for the incremental learning scenario:

$$Performance_{Fixed} = f\left(M_{Fixed}, D_{\text{Fixed}}\right) \tag{14}$$

As such we considered the following metrics in each performance assessment:

- Accuracy: the ratio of correctly predicted instances (both true positives and true negatives) to the total number of instances, calculated as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{15}$$

  where:

  - TP (True Positives): Correctly identified instances.
  - TN (True Negatives): Correctly rejected instances.
  - FP (False Positives): Incorrectly identified instances.
  - FN (False Negatives): Incorrectly rejected instances.

- Precision: the ratio of correctly predicted positive instances to the total predicted positive. In other words, it determines how many of the instances predicted by the model to be a specific person (positive predictions) were actually correct. Precision is useful in biometric security where unauthorized access must be minimized.

$$\text{Precision} = \frac{TP}{TP + FP} \tag{16}$$

- Recall (Sensitivity): the ratio of correctly predicted positive instances to all actual positives. It is another critical parameter for assessing ML models for personal identification as it assesses the model's ability to accurately identify all instances of the target person.

$$\text{Recall} = \frac{TP}{TP + FN} \tag{17}$$

- F1-score: the harmonic mean of precision and recall, providing a balance between the two, especially in case of uneven class distribution. It is especially beneficial in biometric systems as we need to assess both the accuracy (precision) and completeness of positive predictions (recall).

$$F1 - score = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{18}$$

- False Acceptance Rate (FAR): the proportion of incorrect positive identifications (i.e., when an impostor is accepted as a genuine user).

$$\text{FAR} = \frac{\text{Number of False Acceptances}}{\text{Total Number of Impostor Attempts}} \tag{19}$$

  FAR is crucial in biometrics to minimize unauthorized access.
- True Acceptance Rate (TAR): the proportion of correctly accepted genuine user attempts. It is synonymous with Recall or Sensitivity.

$$\text{TAR} = \frac{\text{Number of True Acceptances}}{\text{Total Number of Genuine Attempts}} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{20}$$

  TAR is used to measure the accuracy of a system in correctly identifying legitimate users.
- False Positive Rate (FPR): the proportion of impostor attempts that are incorrectly accepted. This is also referred to as the False Acceptance Rate (FAR) in the biometric context.

$$\text{FPR} = \frac{\text{Number of False Acceptances}}{\text{Total Number of Impostor Attempts}} = \frac{\text{FP}}{\text{FP} + \text{TN}} \tag{21}$$

- False Rejection Rate (FRR): the proportion of genuine user attempts that are incorrectly rejected, which is the complement of the True Acceptance Rate (TAR).

$$\text{FRR} = \frac{\text{Number of False Rejections}}{\text{Total Number of Genuine Attempts}} = \frac{\text{FN}}{\text{TP} + \text{FN}} \tag{22}$$

  The FRR measures how often the system incorrectly rejects legitimate users.

5 Experiments, Results, and Analysis

To assess the performance of our proposed model, we conducted a comprehensive analysis using the various incremental sets shown in Fig. 2: cumulative, incremental, and fixed sets. The analysis compares the performance of our model against two benchmarks: the Naïve approach and the Joint approach.

The Naïve approach serves as a baseline for our evaluation. This method involves training the model incrementally without any mechanisms to retain previously learned information. As each new batch of data is introduced, the model is retrained on only the new data. The Naïve approach is expected to demonstrate a rapid decline in performance on older data as new increments are introduced. This allows us to observe the degree of catastrophic forgetting in our generated scenarios.

On the other hand, the Joint approach represents the traditional deep learning method where the model is trained on all data simultaneously in one batch. This approach represents the upper bound standard for accuracy since it maximizes the available data during training.

First, we evaluated the final accuracy of all models after training on the complete dataset. Both the Naïve approach and our proposed model were trained incrementally, while the Joint approach was tested twice: once with an unoptimized number of epochs (denoted as Joint), and once after hyperparameter optimization (denoted as Joint_200). The optimization process revealed that increasing the number of epochs beyond a certain point led to diminished returns, prompting us to cap the number of epochs at 200 for joint training.

Fig. 4 plots the accuracy results against the number of epochs and highlights the performance trends for all models. The results are shown for models trained in all 31 active classes. The top plot displays the accuracy trend, revealing how catastrophic forgetting and performance stability vary among the strategies. The bottom plot provides a granular comparison of accuracy per increment, emphasizing the differences in model behavior under varied training constraints and resources. This analysis showcases both upper and lower performance bounds. As expected, the Naïve approach exhibits significant catastrophic forgetting, particularly after introducing new data increments. The Naïve model fails to retain any information from previous experiences, with accuracies dropping to nearly zero on past experiences.

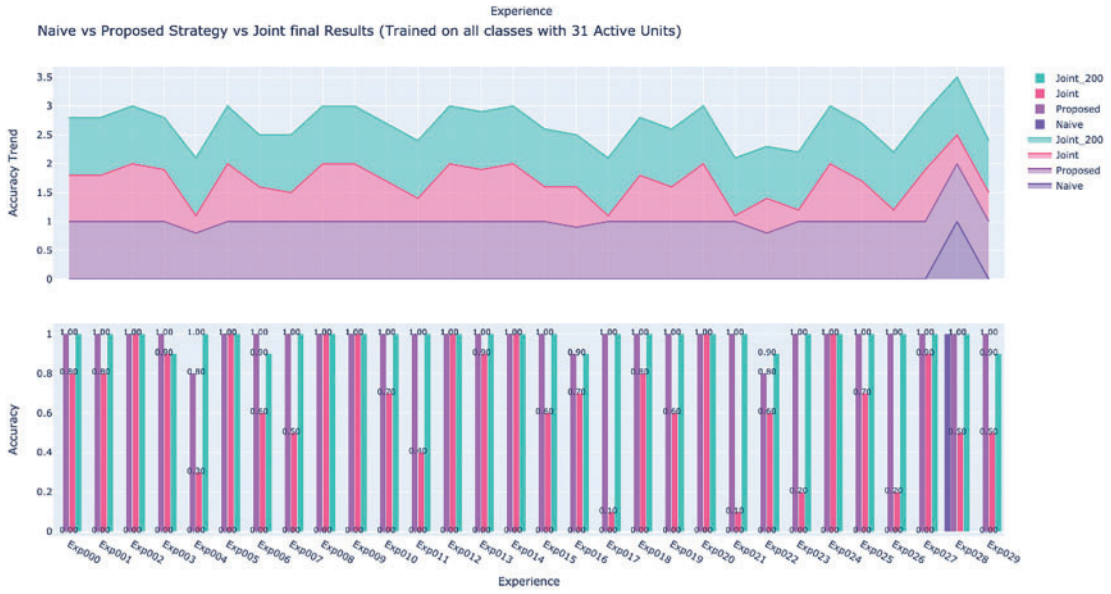

Figure 4: Comparative analysis of model retention capabilities using different training strategies: (Top): accuracy trend over successive increments; (Bottom): detailed breakdown of accuracy per increment

On the other hand, the accuracy trend for our proposed model remains highly competitive with the Joint approaches. Fluctuations of approximately 5%–7% are observed across various increments, as shown in the bar plot. However, the model consistently performs at near-optimal levels, closely aligning with the Joint_200 model, which represents the upper bound in terms of accuracy and stability due to its extensive resource allocations and full data availability. Remarkably, in certain increments, the proposed model even outperforms the Joint Approach, which was trained with the same resource allocation but demonstrated lower identification performance and less stability.

The Joint_200 strategy, while achieving slightly higher accuracy (reaching nearly 100% on the training sets), comes at a significant cost in terms of computational resources and longer training times. In contrast,

our proposed model strikes a strong balance, maintaining high accuracy without the overhead of full retraining, proving its efficiency in managing incremental data.

To further analyze these results, we conducted a more detailed analysis where the models are benchmarked against each increment individually. This highlights how stable and consistent the models are over time. Fig. 5 plots the incremental strategies' results against the Joint Strategy, providing insights into how the models perform as more data is introduced.

Figure 5: Performance comparison between incremental learning and batch learning under increasing complexity: (Top): illustrates the training accuracy and active unit evolution for various incremental learning strategies with each training experience; (Bottom): illustrates the performance of traditional batch learning methods using two Joint strategies

Fig. 5 shows the performance of Incremental Strategies (top graph) compared with the Joint Strategy (bottom graph) across different training experiences. Unlike the previous analysis, which focused on backward transfer and adaptability capabilities, this figure illustrates the performance and stability of each strategy as it adapts to new data increments. Importantly, the results of incremental strategies are collected immediately after each increment, rather than using the last model with 31 active units.

The proposed model shows impressive stability, with accuracy remaining close to 100% across nearly all increments. It demonstrates competitive accuracy and stability when compared to the hyperparameter-tuned Joint_200 model.

The number of active units increases as new users enroll (representing the growing complexity of the task); however, the proposed model was capable of maintaining high accuracy rates, with minimal fluctuations, showcasing its capability to handle incremental learning without significant loss of performance. In contrast, the Naïve Strategy, which was capable of reaching comparable results (highlighting the performance of our proposed 1D-CNN architecture), suffers from sharp drops in accuracy after certain increments. As complexity grows, these drops become more frequent.

Interestingly, similar to the Naïve model, the Joint Strategy also experiences occasional dips in accuracy, despite having access to the full dataset during each training scenario. These fluctuations suggest that even full

retraining does not guarantee perfect stability, especially when the model is trained with limited resources, as indicated by the Joint strategy (20 epochs) sharing similar resources with our proposed model.

We further assess the retention capabilities of our model by evaluating its performance in cumulative scenarios, which differ from testing on individual increments (i.e., testing on a single individual after learning). The cumulative approach tests the model on all previously learned individuals after being introduced to a new cumulative set. This method provides a more comprehensive view of retention across multiple increments and better captures the complexity of real-world applications, where a model must adapt to new instances and retain knowledge from various experiences simultaneously, simulating more realistic conditions. For instance, after being exposed to individual number 6, the model is tested on individuals 0 to 6. After learning up to 12 individuals, the model is tested on individuals 0 to 12, and so forth, until the model has been exposed to the entire dataset. This holistic evaluation challenges the model to retain more complex sets of knowledge while also testing how well it integrates new information without forgetting previously learned data.

Fig. 6 illustrates the performance of the proposed approach compared to the Naïve strategy in cumulative testing scenarios. Cumulative testing evaluates whether the model retains previously learned individuals as more increments are introduced, simulating real-world conditions. The Naïve strategy demonstrates the expected effects of catastrophic forgetting, where earlier learned individuals are no longer recognized due to the model's strictly sequential learning approach. In contrast, the proposed strategy maintains consistently high accuracy around 98%, adapting to new data while retaining prior knowledge. The observed drop in Naïve strategy performance may seem extreme but is consistent with incremental learning settings where no knowledge retention mechanisms are used. At each increment, the model fully adapts to the most recent data, overwriting previously learned patterns. This effect is particularly evident in the final stages of training, where the model has last seen only a single user, reinforcing class-specific overfitting at the expense of prior generalization. While reducing training epochs in the Naïve approach could moderate this decline, doing so would alter the benchmark conditions, potentially biasing comparisons between strategies. Additionally, no such overfitting effects were observed in other strategies under the same settings, supporting that the observed decline is due to catastrophic forgetting rather than experimental irregularities.

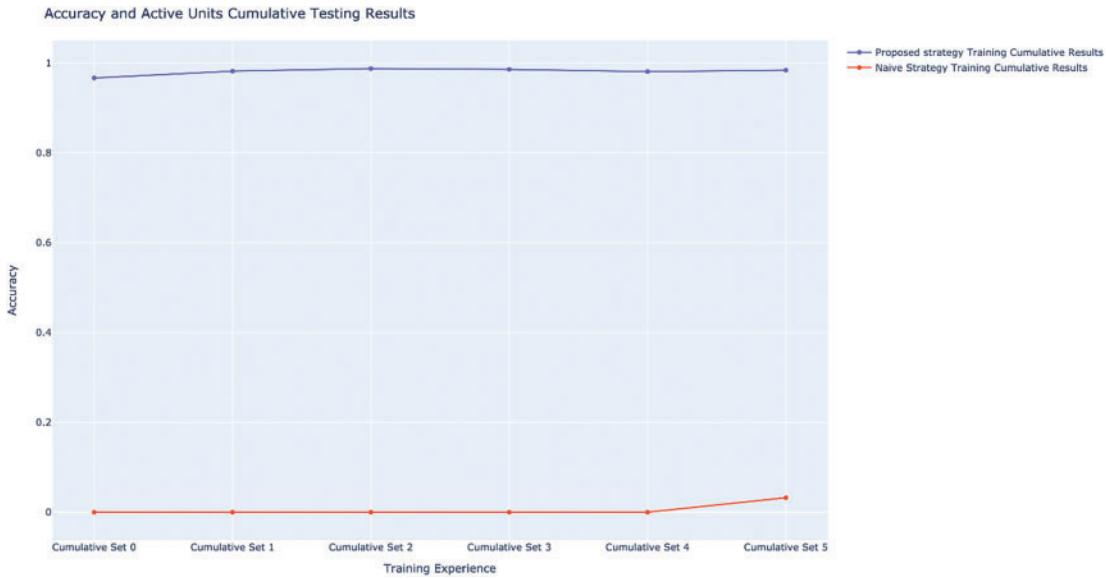

Figure 6: Retention analysis of the proposed model on cumulative test sets

Now, we evaluate our framework's biometric capabilities. Table 3 depicts the detailed values of these metrics for each cumulative test set.

Table 3: Proposed model's biometric recognition performance analysis across all cumulative sets

EXP_ID	FAR	TAR	FPR	FRR	ROC-AUC	Accuracy	Precision (Avg)	Recall (Avg)	F1-score (Avg)
4—(0–5)	0.0033	0.9833	0.0033	0.0167	0.9967	0.9833	0.984848	0.983333	0.983292
9—(0–10)	0.0027	0.9727	0.0027	0.0273	0.9973	0.9727	0.979021	0.972727	0.9721
14—(0–15)	0	1	0	0	1	1	1	1	1
19—(0–20)	0.0005	0.9905	0.0005	0.0095	0.9995	0.9905	0.991342	0.990476	0.990452
24—(0–25)	0.0003	0.9923	0.0003	0.0077	0.9997	0.9923	0.993007	0.992308	0.992288
29—(0–30)	0.0001	0.9968	0.0001	0.0032	0.9999	0.9968	0.99697	0.996774	0.996766

The biometric evaluation yields highly promising results, consistently achieving an average accuracy of 98.92% as the dataset expands with additional individuals. Notably, the FAR remains impressively low at an average of 0.00115, while the TAR remains high at approximately 0.9893.

Additionally, the precision, recall, and F1-score hover around 98.98%, demonstrating that the system not only produces accurate predictions but also maintains an excellent balance between precision/FPR (minimizing false positives) and recall/FRR (minimizing false negatives). This balance is particularly important in biometric systems, where both false positives (incorrectly accepting an impostor) and false negatives (incorrectly rejecting a legitimate user) can have significant security and usability implications.

Finally, the near-perfect Area Under the Receiver Operating Characteristic Curve (ROC-AUC) analysis further emphasizes the model's strong discriminatory capabilities, effectively balancing the trade-off between the TAR (or TPR) and FPR. Most importantly, this high level of distinction is consistently maintained across all cumulative sets and even shows improvement as the model is exposed to more individuals over time. This highlights the proposed architecture's adaptability and capacity to adapt effectively, even as complexity increases.

While exact quantitative comparisons are limited due to differing datasets, experimental setups, and varying research objectives, the reported accuracy and F1 ranges provide a useful contextual benchmark for evaluating general performance trends in the field. Our analysis demonstrates that the proposed model achieves a strong balance between scalability and accuracy. For instance, methods reported in [26,24], and [22] achieved accuracies of 86%–93%, 94.12%, and 96%–97.6% (upper bound) respectively, with overall ranges in the literature between 85% and 96%. Similarly, authors in [29] reported an F1 measure of 94%, maintaining robustness until 60% openness.

In contrast, our model consistently achieved an average accuracy of 98.92% as the dataset expanded with additional individuals. Furthermore, it maintained an average F1-score of 98.91% across different increments, reaching 99.67% in the largest increment. These results underscore the effectiveness of our approach in handling incremental data growth, performing competitively with, and in some cases surpassing, parallel research in the field.

6 Conclusion and Future Work

In this paper, we presented a novel approach that addresses the challenges of scalability and security in biometric recognition systems. At the design level, we proposed a unified framework for enrollment and identification that encompasses deep feature extraction using ResNet-50 from face and fingerprint

datasets, biometric traits fusion, cancelable template generation using random projection, and a 1D-CNN dynamic architecture that can accommodate a growing user base. Incremental learning is achieved via a joint contribution of the dynamic architecture of the 1D-CNN, the elastic weight regularization mechanism, and the incorporation of a rehearsal strategy based on the use of reservoir sampling to allow the model to learn from a mixture of old and new increments during incremental training. Based on this proposed framework three models have been designed to handle three scenarios to investigate the incremental learning capabilities of the proposed approach. The first model trained on fixed sets with two variants, the second model trained on cumulative sets, and the third model trained on incremental sets.

At the implementation and evaluation level, a comprehensive experimental study has been conducted to assess the performance of the proposed approach while ensuring the reliability of the results. This has required conducting several experiments related to the aforementioned three scenarios and using several performance metrics. Also, as a comparative study, we set the lower bound using a Naïve learning strategy and the upper bound using a Joint strategy under two conditions: resource-limited and unbound resources (200 epochs). At the results level, the evaluation of our biometric identification framework demonstrates highly promising results, consistently achieving an average accuracy of 98.92% across all testing benchmarks. Moreover, our system achieves a very low FAR averaging 0.00115, and a high TAR of approximately 0.9893. Additionally, precision, recall, and F1-score all hover around 98.98%. This approach stands out for its capability to achieve high retention rates, even as system complexity increases with additional users. The system successfully leverages hybrid incremental learning approaches to mitigate the issue of catastrophic forgetting. Moreover, it integrates a small overhead layer for security by utilizing a low-performance-demanding random projection algorithm to generate cancelable templates. As such, this framework not only achieves a strong balance between scalability, accuracy, and incremental learning but also optimizes resource utilization while consistently achieving near-perfect (1.0) AUC-ROC scores.

In future work, the scalability of the system can be evaluated on significantly larger datasets and with a much higher number of classes to fully assess its robustness in real-world scenarios. While the datasets used in this study were chosen for their suitability in testing under controlled conditions, the current scope is limited to 31 classes and a rehearsal buffer of 1000 samples. These parameters were sufficient to demonstrate the framework's effectiveness within the research context. However, as the number of users and classes grows, it is critical to analyze whether performance degradation occurs and how the rehearsal buffer can scale effectively to accommodate larger populations. This investigation would also help refine the trade-offs between buffer size, computational cost, and performance.

The rehearsal buffer itself poses unique challenges beyond scalability. While it is more secure than storing raw biometric data—since it only retains cancellable templates—and is deeply integrated with the recognition model, its security in deployment environments still must be thoroughly evaluated. Future research should explore mechanisms to protect the buffer from potential attacks, such as data poisoning or model inversion. Balancing these security measures with the system's adaptability will be key to maintaining its efficiency. Further exploration of incremental learning methods could address these challenges by minimizing reliance on stored data while preserving the model's ability to adapt to new data. Additionally, addressing challenges in identification lays the foundation for more robust authentication processes. Therefore, future research will aim to expand upon our current findings by incorporating authentication mechanisms [41]. On another side, although the integration of random projection with deep features substantially enhances the security of biometric systems, it is not entirely immune to certain sophisticated attacks, Including reconstruction attacks, adversarial attacks, and template matching attacks [42]. To further fortify the robustness of this combined approach, it is advisable to augment random projection with additional cancelable biometric techniques, such as permutation-based methods or feature domain

transformations [43]. This multi-layered security architecture would provide a more comprehensive defense mechanism, addressing a broader spectrum of potential vulnerabilities and ensuring a higher level of protection for biometric data. Therefore, investigation of the impact of various cancelable templates would provide a more comprehensive analysis of biometric security systems as a whole. Finally, the system's deployment should be analyzed on resource-constrained devices to evaluate latency, computational efficiency, and storage requirements. By addressing these interconnected limitations, the framework can evolve to support larger-scale deployments while maintaining security, efficiency, and scalability.

Acknowledgement: None.

Funding Statement: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through project number RI-44-0833.

Author Contributions: The authors confirm their contribution to the paper as follows: Conceptualization, Souham Meshoul, Ali Batouche, and Mohamed Batouche; methodology, Souham Meshoul, Ali Batouche, Hadil Shaiba, and Mohamed Batouche; software, Ali Batouche; validation, Souham Meshoul, Ali Batouche, and Mohamed Batouche; writing—original draft preparation, Ali Batouche, Souham Meshoul, Mohamed Batouche, and Hadil Shaiba; writing—review and editing, Souham Meshoul, Ali Batouche, Hadil Shaiba, and Mohamed Batouche; visualization, Ali Batouche; supervision, Mohamed Batouche; funding acquisition, Souham Meshoul. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are openly available in Kaggle [30,31].

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Ghilom M, Latifi S. The role of machine learning in advanced biometric systems. Electronics. 2024 Jul 7;13(13):2667. doi:10.3390/electronics13132667.
2. Hemis M, Kheddar H, Bourouis S, Saleem N. Deep learning techniques for hand vein biometrics: a comprehensive review. Inf Fusion. 2025 Feb;114(32):102716. doi:10.1016/j.inffus.2024.102716.
3. Manisha, Kumar N. Cancelable biometrics: a comprehensive survey. Artif Intell Rev. 2020 Jun;53(5):3403–46. doi:10.1007/s10462-019-09767-8.
4. Geng C, Huang SJ, Chen S. Recent advances in open set recognition: a survey. IEEE Trans Pattern Anal Mach Intell. 2021 Oct;43(10):3614–31. doi:10.1109/TPAMI.2020.2981604.
5. Smith-Creasey M. Continuous biometric authentication systems. In: SpringerBriefs in computer science. Cham: Springer International Publishing; 2024 [cited 2024 Nov 22]. p. 1–4. Available from: https://link.springer.com/10.1007/978-3-031-49071-2_1.
6. Ratha NK, Connell JH, Bolle RM. Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J. 2001;40(3):614–34. doi:10.1147/sj.403.0614.
7. Wang Y, Shi D, Zhou W. Convolutional neural network approach based on multimodal biometric system with fusion of face and finger vein features. Sensors. 2022 Aug 12;22(16):6039. doi:10.3390/s22166039.
8. Micucci M, Iula A. Recognition performance analysis of a multimodal biometric system based on the fusion of 3D ultrasound hand-geometry and palmprint. Sensors. 2023 Mar 31;23(7):3653. doi:10.3390/s23073653.
9. Wang L, Zhang X, Su H, Zhu J. A comprehensive survey of continual learning: theory, method and application. IEEE Trans Pattern Anal Mach Intell. 2024 Aug;46(8):5362–83. doi:10.1109/TPAMI.2024.3367329.

10. Lesort T, Lomonaco V, Stoian A, Maltoni D, Filliat D, Díaz-Rodríguez N. Continual learning for robotics: definition, framework, learning strategies, opportunities and challenges. Inf Fusion. 2020 Jun;58(10–12):52–68. doi:10.1016/j.inffus.2019.12.004.
11. Chaudhry A, Dokania PK, Ajanthan T, Torr PHS. Riemannian walk for incremental learning: understanding forgetting and intransigence. In: Ferrari V, Hebert M, Sminchisescu C, Weiss Y, editors. Computer vision—ECCV 2018 [Internet]; Cham: Springer International Publishing; 2018 [cited 2024 Sep 26]; p. 556–72. Available from: https://link.springer.com/10.1007/978-3-030-01252-6_33.
12. Lopez-Paz D, Ranzato M. Gradient episodic memory for continual learning. arXiv:1706.08840. 2017.
13. Minaee S, Abdolrashidi A, Su H, Bennamoun M, Zhang D. Biometrics recognition using deep learning: a survey. Artif Intell Rev. 2023 Aug;56(8):8647–95. doi:10.1007/s10462-022-10237-x.
14. Abdellatef E, Omran EM, Soliman RF, Ismail NA, Abd Elrahman SESE, Ismail KN, et al. Fusion of deep-learned and hand-crafted features for cancelable recognition systems. Soft Comput. 2020 Oct;24(20):15189–208. doi:10.1007/s00500-020-04856-1.
15. Abdellatef E, Ismail NA, Abd Elrahman SESE, Ismail KN, Rihan M, Abd El-Samie FE. Cancelable fusion-based face recognition. Multimed Tools Appl. 2019 Nov;78(22):31557–80. doi:10.1007/s11042-019-07848-y.
16. Bansal V, Garg S. A cancelable biometric identification scheme based on bloom filter and format-preserving encryption. J King Saud Univ—Comput Inf Sci. 2022 Sep;34(8):5810–21. doi:10.1016/j.jksuci.2022.01.014.
17. Bernal-Romero JC, Ramirez-Cortes JM, Rangel-Magdaleno JDJ, Gomez-Gil P, Peregrina-Barreto H, Cruz-Vega I. A review on protection and cancelable techniques in biometric systems. IEEE Access. 2023;11(5):8531–68. doi:10.1109/ACCESS.2023.3239387.
18. Yongjin W, Plataniotis KN. An analysis of random projection for changeable and privacy-preserving biometric verification. IEEE Trans Syst, Man, Cybern B. 2010 Oct;40(5):1280–93. doi:10.1109/TSMCB.2009.2037131.
19. Kim J, Yang G, Kim J, Lee S, Kim KK, Park C. Efficiently updating ECG-based biometric authentication based on incremental learning. Sensors. 2021 Feb 24;21(5):1568. doi:10.3390/s21051568.
20. Universiti Malaysia Sarawak, Anak Joseph A, Anak Pelias Pog EI, Universiti Malaysia Sarawak, Chin KL, Universiti Malaysia Sarawak et al. Online person identification based on multitask learning. IJIE [Internet]. 2021 Feb 11 [cited 2024 Sep 25];13(2). Available from: https://publisher.uthm.edu.my/ojs/index.php/ijie/article/view/6613/3913.
21. Singh A, Vashist C, Gaurav P, Nigam A. A generic framework for deep incremental cancelable template generation. Neurocomputing. 2022 Jan;467(3):83–98. doi:10.1016/j.neucom.2021.09.055.
22. Agarwal S, Rattani A, Chowdary CR. A-iLearn: an adaptive incremental learning model for spoof fingerprint detection. Mach Learn Appl. 2022 Mar;7(12):100210. doi:10.1016/j.mlwa.2021.100210.
23. Peralta D, Triguero I, García S, Saeys Y, Benitez JM, Herrera F. Distributed incremental fingerprint identification with reduced database penetration rate using a hierarchical classification based on feature fusion and selection. Knowl Based Syst. 2017 Jun;126(2):91–103. doi:10.1016/j.knosys.2017.03.014.
24. Mehrotra H, Singh R, Vatsa M, Majhi B. Incremental granular relevance vector machine: a case study in multimodal biometrics. Pattern Recognit. 2016 Aug;56(4):63–76. doi:10.1016/j.patcog.2015.11.013.
25. Mu Z, Castro FM, Marin-Jimenez MJ, Guil N, Li YR, Yu S. iLGaCo: incremental learning of gait covariate factors. In: 2020 IEEE International Joint Conference on Biometrics (IJCB) [Internet]; 2020 [cited 2024 Nov 22]; Houston, TX, USA: IEEE. p. 1–8. Available from: https://ieeexplore.ieee.org/document/9304857/.
26. Kang J, Lu N, Niu X. Incremental EEG biometric recognition based on EEG relation network. In: Deng W, Feng J, Huang D, Kan M, Sun Z, Zheng F et al., editors. Biometric recognition [Internet]. Cham: Springer Nature Switzerland; 2022 [cited 2024 Nov 22]. p. 424–32. Available from: https://link.springer.com/10.1007/978-3-031-20233-9_43.
27. Zhou L, Oechtering TJ, Skoglund M. Incremental design of secure biometric identification and authentication. In: 2021 IEEE International Symposium on Information Theory (ISIT) [Internet]; 2021 [cited 2024 Nov 22]; Melbourne, Australia: IEEE. p. 3196–201. Available from: https://ieeexplore.ieee.org/document/9518285/.
28. Shen Z, Li S, Zhao X, Zou J. IncreAuth: incremental-learning-based behavioral biometric authentication on smartphones. IEEE Internet Things J. 2024 Jan 1;11(1):1589–603. doi:10.1109/JIOT.2023.3289935.

29. Lopez-Lopez E, Pardo XM, Regueiro CV. Incremental learning from low-labelled stream data in open-set video face recognition. Pattern Recognit. 2022 Nov;131(12):108885. doi:10.1016/j.patcog.2022.108885.
30. Shehu YI, Ruiz-Garcia A, Palade V, James A. Sokoto coventry fingerprint dataset [Internet]. arXiv:1807.10609. 2018.
31. Face recognition dataset [Internet]. [cited 2024 Sep 26]. Available from: https://www.kaggle.com/datasets/vasukipatel/face-recognition-dataset.
32. Gold S. Iris biometrics: a legal invasion of privacy? Biom Technol Today. 2013 Mar;2013(3):5–8.
33. Hassan B, Izquierdo E, Piatrik T. Soft biometrics: a survey: benchmark analysis, open challenges and recommendations. Multimed Tools Appl. 2021 Mar 2;83(5):15151–94. doi:10.1007/s11042-021-10622-8.
34. Arpit D, Nwogu I, Srivastava G, Govindaraju V. An analysis of random projections in cancelable biometrics [Internet]. 2014 [cited 2025 Feb 1]. Available from: https://arxiv.org/abs/1401.4489.
35. Dasgupta S, Gupta A. An elementary proof of a theorem of Johnson and Lindenstrauss. Random Struct Algorithms. 2003 Jan;22(1):60–5. doi:10.1002/rsa.10073.
36. Almondo4/BioIncremt [Internet]. GitHub. [cited 2025 Jan 4]. Available from: https://github.com/Almondo4/BioIncremt.
37. Carta A, Pellegrini L, Cossu A, Hemati H, Lomonaco V. Avalanche: a pytorch library for deep continual learning. J Mach Learn Res. 2023;24(363):1–6.
38. Lomonaco V, Pellegrini L, Cossu A, Carta A, Graffieti G, Hayes TL, et al. Avalanche: an end-to-end library for continual learning. In: 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) [Internet]. Nashville, TN, USA: IEEE; 2021. p. 3595–605. [cited 2025 Mar 13]. Available from: https://ieeexplore.ieee.org/document/9523188/.
39. Kirkpatrick J, Pascanu R, Rabinowitz N, Veness J, Desjardins G, Rusu AA, et al. Overcoming catastrophic forgetting in neural networks. 2016 [cited 2023 Aug 12]. Available from: https://arxiv.org/abs/1612.00796.
40. Aggarwal CC. On biased reservoir sampling in the presence of stream evolution. In: Proceedings of the 32nd International Conference on Very Large Data Bases; 2006; Seoul, Republic of Korea: VLDB Endowment. p. 607–18.
41. Boshoff D, Hancke GP. A classifications framework for continuous biometric authentication (2018–2024). Comput Secur. 2025 Mar;150(5):104285. doi:10.1016/j.cose.2024.104285.
42. Abdullahi SM, Sun S, Wang B, Wei N, Wang H. Biometric template attacks and recent protection mechanisms: a survey. Inf Fusion. 2024 Mar;103(2):102144. doi:10.1016/j.inffus.2023.102144.
43. Abdullahi SM, Lv K, Sun S, Wang H. Cancelable fingerprint template construction using vector permutation and shift-ordering. IEEE Trans Dependable Secure Comput. 2023 Sep 1;20(5):3828–44. doi:10.1109/TDSC.2022.3213704.