ISSN 2278-3091
Volume 13, No.6, November - December 2024
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse081362024.pdf
https://doi.org/10.30534/ijatcse/2024/081362024

A Fingerprint-Based Neural Network Approach for Age Estimation in Young Adults

Oladayo O. Amusan[1], Amarachi M. Udefi[2], Safiriyu I. Eludiora[3]
[1]Obafemi Awolowo University, Ile-Ife, Osun State, 220282, Nigeria, dayoamusan49@gmail.com
[2]Grundtvig Polytechnic Oba, Anambra State, Nigeria, Amarachi.udefi@grundtvigpolytechnic.com
[3]Obafemi Awolowo University, Ile-Ife, Osun State, 220282, Nigeria, safiriyue@yahoo.com

Received Date: October 15, 2024 Accepted Date: November 23, 2024 Published Date: December 06, 2024

ABSTRACT

Age estimation using biometric data is a critical tool in various applications, ranging from security systems to age-based access control in digital platforms. This study presents the development of a fingerprint-based age estimation system for individuals aged 15–23 years. The system captures fingerprint data using a USB-connected scanner, preprocesses the data, and utilizes a Counter-Propagation Neural Network (CPNN) trained with Grossberg's learning rule for classification. A dataset of 500 fingerprint samples was collected, and the system's performance was evaluated using metrics such as accuracy, sensitivity, and specificity across different threshold values. The system achieved a maximum accuracy of 96%, sensitivity of 94%, and specificity of 95% at a threshold of 0.7, demonstrating its effectiveness in age classification. Challenges, particularly in borderline cases, highlight the need for further refinement of the feature extraction and classification process. This study highlights the feasibility of using biometric data for age estimation, with potential applications in forensics, access control, and demographic studies. The results provide a foundation for future work on improving system performance and scalability by incorporating advanced feature extraction techniques and larger, more diverse datasets.

Key words: Fingerprint biometrics, age estimation, counter-propagation neural network, sensitivity analysis, machine learning, Grossberg learning rule.

1. INTRODUCTION

Age is a predominant factor in our society, influencing activities such as job recruitment, sports, elections, and age-restricted transactions. It plays a significant role in everyday life and represents a developmental process involving both gains and losses [3]. Accurate age is important to determine potential resources for dealing with stressful life events. It is also important to attain milestones of development [7]. For local authorities to fulfill their obligations, accurate age estimation is important. This will also help in the proper administration of support and services to children less than 18 years old [7]. To estimate age, specialized software that utilizes fingerprint readers is required. Similar to other systems, age estimation systems process an input, whether biometric data, teeth, or bones, and analyze it to determine an individual's age [13].

Biometrics refers to the use of unique physical or behavioral characteristics of the human body to identify individuals or objects. This method of authentication is considered more reliable than traditional approaches such as passwords, registration numbers, ID cards, or smart cards. Unlike passwords, which can be forgotten, or smart cards, which can be misplaced, biometric identifiers are inherent to the individual, making them more secure and convenient.

Age estimation using biometric data is a critical tool in various applications, ranging from security systems to age-based access control in digital platforms [13]. Among biometric modalities, fingerprints offer a unique and non-invasive method of identification and analysis, given their stability over time and widespread use in identification systems. While extensive research has explored fingerprint-based identification, the potential of fingerprints for age estimation remains an underexplored domain, particularly for adolescents and young adults.

[2] participation in athletic sports is closely regulated by the age of the athletes. For example, youth sports require age verification, and Olympic events enforce minimum age requirements. Research has shown that social factors such as culture, age, and gender can both restrict and enhance participation in sports [17]. The physical nature of sports is also influenced by aging, as age-related changes can impact an athlete's ability to compete. These changes may affect training demands, competition schedules, and overall physical performance.

Even slight inaccuracies in age estimation can lead to adults being denied the freedoms associated with adulthood, while children may be expected to act in ways that do not align with their true age. This is particularly evident in children who have experienced malnutrition or severe trauma, as they may undergo a growth spurt with accelerated skeletal maturation once they settle in environments like Australia. Their physical and sexual maturation may also progress more quickly [7].

This study addresses the challenge of estimating ages within a narrow range of 15 to 23 years, a period characterized by subtle biometric changes. Existing methods often struggle to achieve high accuracy within such a confined range, particularly with datasets comprising real-world variability. The research focuses on designing and implementing an age estimation system leveraging fingerprint data and a counter-propagation neural network, trained using Grossberg's learning rule.

The proposed system captures fingerprints using a USB-interfaced scanner and stores them in a database for preprocessing and neural network training as shown in Figure 1. Performance metrics such as specificity, sensitivity, and accuracy are analyzed across varying thresholds to identify optimal system parameters. Results demonstrate that the system achieves a maximum accuracy of 96% at a threshold of 0.7, highlighting its potential for practical applications in age verification systems. This paper contributes to the field by demonstrating the feasibility of fingerprint-based age estimation within a specific demographic, paving the way for further research into fine-grained biometric age analysis. The findings have implications for industries requiring precise age verification methods, such as digital identity verification and legal age enforcement.

The paper is organized as follows: Literature Review is treated in Section II. Section III describes the methodology used in the development of the fingerprint-based Neural Network system, the result and discussion are in Section IV; Section V shows the conclusion while Section VI is the future work of fingerprint biometric age verification.

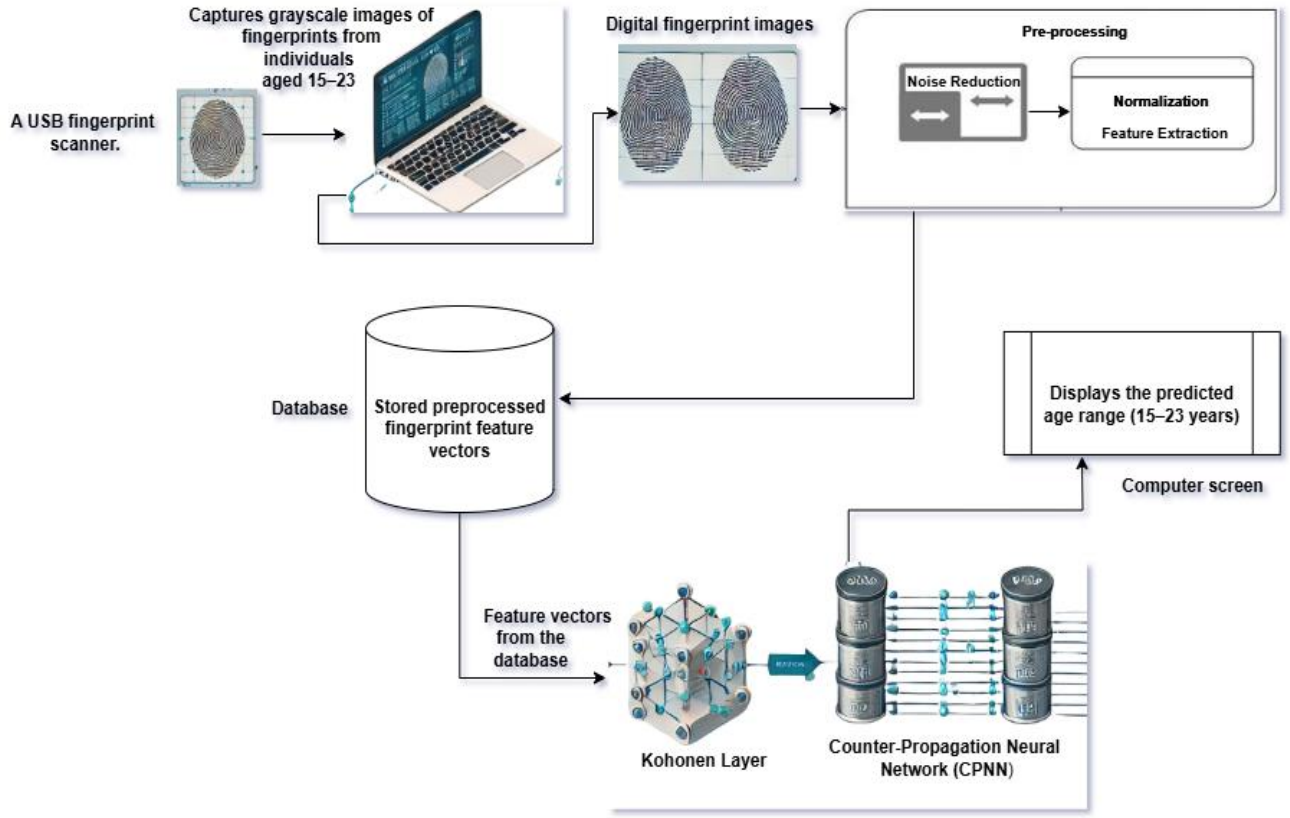

Figure 1: Developed System

2. LITERATURE REVIEW

2.1. Biometrics

Biometrics refers to the measurement of distinctive physical or behavioral characteristics to confirm an individual's identity. Physical biometrics commonly include fingerprints, palm geometry, and features of the retina, iris, or face, while behavioral biometrics cover aspects such as voice, signature, keystroke dynamics, and gait. These technologies are extensively employed for access control and have substantial applications in privacy- and security-focused sectors like stadiums, airports, defense facilities, industries, and corporate environments [26].

2.1.1. Face

Facial recognition is a dependable and secure method that uses facial features such as the eyebrows, lips, eyes, nose, and chin to identify individuals. The process involves analyzing facial images to extract distinctive characteristics. For a facial recognition system to function effectively, it must accurately detect a face in the captured data, identify it, and recognize it from different angles and under varying environmental conditions [21], [32].

2.1.2. Hand geometry

Hand geometry-based authentication systems use measurements of the human hand, such as palm shape, finger lengths, and widths [24]. These systems are popular in various settings due to their simplicity, ease of use, and cost-effectiveness. Environmental factors, such as dry weather, and personal conditions, like dry skin, generally do not impact their accuracy. However, hand geometry lacks distinctiveness, making these systems unsuitable for identifying individuals within large populations. Additionally, hand geometry can change during childhood growth, and factors such as jewelry (e.g., rings) or physical conditions (e.g., arthritis) may interfere with accurate measurements. The physical size of these systems is also a limitation, preventing their integration into smaller devices like laptops. To address this, smaller authentication systems focusing on measurements from a few fingers, typically the index and middle fingers, have been developed. While more compact than full-hand systems, they remain larger than devices used for other biometric traits, such as fingerprint, facial recognition, or voice authentication.

2.1.3. Iris

The visual texture of the iris forms during fetal development and stabilizes within the first two years of life, though its pigmentation may continue to change over time. This intricate texture contains highly distinctive information, making it valuable for personal recognition. Modern iris-based recognition systems are highly accurate and efficient, supporting their use in large-scale identification systems [18]. Each iris is unique, even among identical twins, and these systems can detect contact lenses with fake iris patterns. The natural hippus movement of the eye can be used as a liveness detection measure in iris-based biometrics. While early iris recognition systems were expensive and demanded significant user involvement, modern systems are more affordable and user-friendly. Iris recognition systems have a notably low False Accept Rate (FAR) compared to other biometric methods, although their False Reject Rate (FRR) can still be relatively high.

2.1.4. Keystroke

Keystroke dynamics, a behavioral biometric, is not inherently unique to each individual but provides enough discriminatory information for identity verification. Typing patterns can exhibit significant variability within the same person due to factors such as emotional state, user posture, and the type of keyboard used. This biometric can be monitored unobtrusively while a person types, allowing for continuous identity verification throughout a session [16]. It is often used as a supplementary biometric, complementing stronger methods like fingerprint or iris recognition during the initial login process.

2.1.5. Signature

Signatures, unique to each individual, have long served as a means of authentication in government, legal, and commercial transactions. Despite requiring user effort and contact with a writing instrument, they remain widely accepted. With the growing use of PDAs and tablet PCs, online signatures are becoming a preferred biometric for these devices [1]. As a behavioral biometric, signatures can evolve and are influenced by the signer’s physical and emotional state. For some, signatures may vary significantly, even between successive impressions. Moreover, skilled forgers can replicate signatures convincingly enough to bypass verification systems

2.1.6. Voice

Voice recognition utilizes both physical and behavioral characteristics of biometric data. The physical aspects, determined by unique and invariant vocal structures such as the vocal tract, mouth, nasal cavities, and lips, distinguish individuals [19]. In contrast, behavioral aspects, including speech patterns, can vary over time due to factors like aging, medical conditions (e.g., a cold), or emotional state. Voice recognition systems may be text-dependent, requiring a specific phrase, or text-independent, identifying the speaker regardless of their speech content. While text-independent systems offer enhanced fraud protection, they are more complex to design. Voice, however, is not highly distinctive, making it less suitable for large-scale identification. Additionally, voice-based recognition is sensitive to factors like background noise and degraded quality in communication channels, though it remains effective for telephone-based applications.

2.1.7. Gait

Gait, the way an individual walks, is one of the few biometric traits that can be used to identify people from a distance, making it particularly useful in surveillance scenarios. Gait recognition systems typically analyze the human silhouette to extract spatiotemporal attributes of movement, with the choice of a robust model for representing the human body being crucial to their effectiveness [29]. Some algorithms utilize the optical flow of dynamically tracked points on the body to characterize an individual's gait. These systems also enable long-term tracking of individuals. However, various factors can influence gait, including footwear, clothing, leg injuries, and the walking surface, which may affect the system's reliability.

2.1.8. Fingerprint

Fingerprint recognition provides highly accurate identification capabilities. A fingerprint is defined by the unique pattern of ridges and valleys on a fingertip, established during the first seven months of fetal development [13]. Research has demonstrated that fingerprints are distinct even among identical twins and across all fingers of the same individual. Modern fingerprint recognition systems are sufficiently accurate for various applications, particularly in forensics. Using multiple fingerprints, such as the ten-print system employed in IAFIS, enhances reliability and enables large-scale identification involving millions of individuals. However, large-scale systems demand significant computational resources, particularly in identification mode.

2.2. Overview of fingerprint

According to [26], evidence of human fingerprints can be found on archaeological artifacts and historical items. The modern study of fingerprints began in the late 16th century when an anatomy professor observed ridges, spirals, and loops in fingerprints [13]. The first scientific claim of fingerprint individuality was made by Henry Fauld in 1880. Around the same time, Herschel revealed he had been researching fingerprints for over 20 years. In the late 19th century, Galton conducted extensive studies on fingerprints and introduced the concept of matching fingerprints based on minutiae features. A significant advancement occurred in 1899 when Edward Henry developed the Henry System of fingerprint classification.

2.2.1. The Human Fingerprint

A fingerprint is the unique pattern of ridges and valleys on the skin of a fingertip, shaped by a combination of genetic and environmental factors. These ridges evolved to enhance grip and grasping capabilities, and even identical twins have distinct fingerprints [22]. The use of fingerprints for identification dates back to ancient times. In 300 BC, the Chinese used fingerprints on official documents, and by the 14th century, inked fingerprints were used by Chinese merchants to identify children. The science of fingerprinting was formally introduced in India in 1858 by Sir William Herschel to prevent impersonation. Sir Francis Galton later systematized fingerprint classification for criminal identification in 1892, a system refined by Sir Edward Henry in 1899, leading to its formal adoption in England in 1894 [12]. Joao de Barros documented the first recorded use of fingerprinting in 14th-century China, while Alphonse Bertillon developed a body measurement system for criminal identification in the late 19th century. However, Bertillon's method was replaced by fingerprinting after inaccuracies in identification. Karl Pearson advanced biometric research in the early 20th century, applying statistical methods such as correlation and the chi-squared test to biometrics and animal evolution.

The concept of fingerprint age determination has been explored in crime investigations to determine the age of latent fingerprints. Despite early studies, modern scientific techniques for fingerprinting did not emerge until the late 16th century [26]. Since the 1960s, advancements in signature biometric authentication and military research have expanded biometric applications beyond fingerprinting [6]

2.2.2. Historical survey of fingerprint

The advent of computers marked a significant advancement in fingerprint identification, utilizing a subset of Galton Points known as minutiae to develop automated fingerprint technology. In the late 1960s, the rise of computing technology led to the automation of fingerprint identification, driven by the Federal Bureau of Investigation (FBI) to streamline the labor-intensive manual processes [10].

In 1969, the FBI partnered with the National Bureau of Standards (NBS), now known as the National Institute of Standards and Technology (NIST), to automate fingerprint classification, searching, and matching [33]. NIST identified two primary challenges:

- Digitally scanning fingerprint cards and extracting minutiae.
- Efficiently searching and matching minutiae against vast fingerprint repositories.

This collaboration resulted in the development of the M40 algorithm, the first operational fingerprint-matching algorithm, which simplified the search process by narrowing down potential matches for expert evaluation. By 1981, advances in fingerprint technology had enabled the deployment of five Automated Fingerprint Identification Systems (AFIS), revolutionizing fingerprint matching and classification.

2.2.3. Types of finger patterns

Before the advent of automated fingerprint systems, manual classification methods were used to organize fingerprints in large-scale operations. These systems classified fingerprints based on general ridge patterns, such as circular formations, enabling the filing and retrieval of paper records without relying on biographical data like names or birth dates, which could be inaccurate [15]. Notable manual systems included the Vucetich system (used in South America), the Henry system (developed in India and widely adopted in English-speaking countries), and the Roscher Classification System [9]. The Henry classification system identified three fundamental fingerprint ridge patterns as shown in Figure 2:

- Arch: Ridges enter from one side, rise in an arc, and exit the other side.
- Loop: Ridges form a curve and exit on the same side they enter.
- Whorl: Ridges circle around a central point**.**

These patterns often run in families, suggesting they are inherited traits that further divide them into subtypes, including plain and tented arches, radial and ulnar loops, and various whorl subcategories (e.g., plain, double loop, and central pocket whorls).

2.2.4. Mechanism of Obtaining Fingerprint

Before the advent of fingerprint sensors, fingerprints were commonly used for personal identification through traditional inked rolled printing processes. However, the efficiency and accuracy of solid-state fingerprint sensors (live scans) have significantly surpassed those of traditional methods.

Fingerprint verification typically involves three main steps:

- Enrollment: Generating and storing a reference model in the database.
- Threshold Calibration: Matching the reference model with various samples to create genuine and impostor scores and computing the threshold.
- Verification/Testing: Using a smart card, username, or ID (e.g., PIN) to identify which template should be used for comparison. Positive recognition is often the objective in this mode, aiming to prevent multiple individuals from using the same identity.

For the identity establishment of anonymous individuals, the system performs a one-to-many comparison with the stored data. This process succeeds if the sample matches within the pre-set threshold. Identification can be either:

- Negative Recognition: Where the user provides no template-related information.
- Positive Recognition: Where the user specifies the template for comparison.

Biometric systems surpass traditional methods like PINs or passwords by offering more secure and reliable identification, as they use unique physical or behavioral traits that are difficult to replicate or steal.

2.2.5. Feature extraction

A fingerprint comprises ridges (dark lines) and valleys (bright areas) that typically run parallel but sometimes split or end abruptly. On a global scale, the fingerprint pattern exhibits distinctive shapes in specific areas, referred to as singularities or singular regions, which are categorized into three types: loops, deltas, and whorls. The core point, commonly used in some algorithms to pre-align fingerprints, represents the center of the highest loop singularity. At a local level, minutiae are essential features of fingerprint patterns, representing ridge discontinuities such as:

- Terminations: Where a ridge abruptly ends.
- Bifurcations: Where a ridge splits into two.

Due to the difficulty of accurately detecting various minutiae forms, many systems classify minutiae into these two main types, these two types are widely used because they are relatively straightforward to detect and are sufficient for most fingerprint recognition and analysis tasks [5]. The system records the coordinates, ridge orientation, and minutiae type for each minutiae point. This process enables precise minutiae extraction, essential for fingerprint recognition systems [30].

Figure 2: Basic fingerprint patterns (source: [34])

2.2.6. Fingerprint Classification

is nearly impossible, estimated at 1 in 1.9×10^{15} [14]. Globally, fingerprints are widely used in large-scale applications for identification and verification. In databases, the automatic identification of individuals using fingerprints involves matching the input fingerprint against a large dataset, such as the FBI database, which contains around 70 million records [27]. To streamline this process, databases are typically organized into well-defined and consistent classes, enabling the input fingerprint to be compared with a smaller subset. This approach significantly reduces both search time and computational complexity. For instance, criminal investigations require a higher degree of fingerprint match than access control systems.

Ridge endings and bifurcations form distinct point patterns that serve as the foundation for fingerprint grouping methods. These methods rely on identifying a set of descriptive features to enable accurate classification [13]. Once the features are determined, a suitable classification mechanism is selected and optimized. However, traditional fingerprint classification techniques often encounter challenges posed by noise and elastic distortions. To overcome these issues and achieve reliable classification, it is essential to extract features that are resilient to such distortions.

2.2.7. Match score

A fingerprint-matching technique produces a score that reflects the proportion of features shared between the stored and live-scan fingerprints [28]. Matching can utilize features such as minutiae or pores. This process is exemplified by comparing two fingerprint segments, whether from the same finger or different fingers. The number of features identified in these segments, referred to as N_E (enlisted features) and N_C (captured features), often differs. Consequently, the matching algorithm must handle varying sets or configurations of features. For instance, a pore-matching score S_P can be expressed as:

$$S_P = \frac{2n_m - n_n}{N_T} \qquad (1)$$

where $N_T = (N_E - N_C$ = total number of pores in both segments

$n_n =$ Number of pores that match

$n_m =$ Number of pores that do not match

And using

$n_n = N_T = 2n_n$

The pore matching score, S_P can be rewritten as:

$$S_P = \frac{4n_m - N_T}{N_T} \quad (2)$$

A pore match is identified when a pore in the comparison image aligns with the location of an enrolled pore, whereas a mismatch occurs when a detected pore in one image has no corresponding pore in the other. The decision to accept or reject a user's claimed identity depends on the calculated pore-matching score (S_P), which ranges from −1 to +1. A score of +1 signifies perfect alignment of pores between the two image segments. Furthermore, the relative rotation of the segments can be determined by analyzing the angles of corresponding minutiae points, which act as local origins for alignment.

2.3. Related Works

Numerous studies have explored biometric modalities for age estimation, with most efforts focusing on facial features, iris patterns, and voice analysis. However, Fingerprint-based studies have largely emphasized identification and authentication, leaving age estimation a relatively nascent field.

[31] investigated fingerprint-based age estimation by analyzing the relationship between fingerprints and an individual's age using frequency domain and pattern recognition techniques. Their method utilized the unique characteristics of fingerprints as a dependable identification tool. The study integrated a 2D Discrete Wavelet Transform (DWT) with Principal Component Analysis (PCA) to estimate a person's age from their fingerprint. A minimum distance classifier was employed for categorization. The dataset included 400 fingerprints from individuals aged between 12 and 60 years. The experimental results demonstrated high accuracy for the trained dataset, with improved performance as the database population increased for each age category.

The dataset, limited to 400 fingerprints, lacks diversity and may not represent broader populations. A larger, more diverse dataset is essential for robustness. The system performed well on the training data but showed signs of overfitting, with its generalization to unseen data unaddressed, raising concerns about its reliability.

[8] developed a system for estimating human age range and gender through fingerprint analysis. The system utilized a Back Propagation Neural Network (BPNN) for gender classification and combined Discrete Wavelet Transform (DWT) with Principal Component Analysis (PCA) for age classification. A dataset of 280 fingerprint samples from individuals across various age groups and genders was collected, with 140 samples (70 male and 70 female) used to train the system. Age groups were divided into seven ranges: 1–10, 11–20, 21–30, 31–40, 41–50, 51–60, and 61–70 years. Gender classification was based on analyzing the Ridge Thickness to Valley Thickness Ratio (RTVTR) to differentiate male and female fingerprints. The system achieved classification accuracies of 80% for females and 72.86% for males. In age classification, 115 out of 140 subjects (82.14%) were correctly classified into their respective age groups.

These results highlight the system's potential for automated age and gender prediction using fingerprint biometrics, though further improvements may be required to enhance accuracy, particularly for male gender classification.

[4] carried out a study on human age estimation using fingerprint analysis. The method involved feature extraction through 2D-Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA), with classification performed using a Support Vector Machine (SVM). The feature extraction process was conducted in two stages: first, the fingerprint image was processed to generate distinct feature vectors. These individual vectors were then merged into a final feature vector, which was used for classification. The classification of the fingerprint into the respective age group was achieved by comparing the final feature vector with those in the database using the SVM classifier.

The two-step feature extraction process involving DWT and PCA could be computationally expensive, especially when processing large datasets, leading to slower processing times for real-time applications.

[11] conducted an experiment using fingerprints to estimate age groups, categorizing individuals as children, adults, or elderly. The study focused on analyzing the variation in genuine matching score (GMS) differences across different age groups. The goal was to determine whether the age of an individual affects the performance of a biometric system.

The classification into broad age groups (children, adults, elderly) may not provide the precision needed for more detailed or fine-grained age estimation, such as estimating specific ages within these categories.

[15] developed an automatic age estimation approach using deep learning models applied to real-world face images. Their proposed method employed two models: a Convolutional Neural Network (CNN) and a deeper version, of a deep CNN. The study demonstrated that the deep CNN model outperformed the regular CNN, achieving an impressive 93% accuracy in age estimation

While deep CNNs showed superior accuracy, they require substantial computational resources and time for training, which may not be feasible for real-time or low-resource applications.

[35] conducted a study on Age and Ageing in Fingerprint Biometrics, the paper explores how age-related changes affect fingerprint features and the potential for using fingerprints for age estimation. It discusses the physiological changes in skin texture, ridge patterns, and fingerprint quality as individuals age. The study highlights challenges in accurately estimating age from fingerprints, such as the subtlety of age-related changes and variations in fingerprint quality across different populations. The research also identifies methods for

improving age estimation, including the use of advanced image processing and machine learning techniques.

While the paper discusses methods for improving age estimation, the accuracy of these techniques may still not meet the required thresholds for real-world applications.

[25] developed a system for Biometric Recognition of Infants using Fingerprint, Iris, and Ear Biometrics. The study explores the use of various biometric traits—fingerprint, iris, and ear—for recognizing infants. It highlights the challenges involved in infant biometrics due to the rapid physical changes that occur in early life. The study examines how these traits can be used effectively despite the difficulties in acquiring stable, high-quality samples from infants. The paper also discusses the potential for integrating multiple biometric modalities to improve recognition accuracy, particularly in the context of early identification systems.

There are technological challenges in integrating and standardizing the use of different biometric modalities (fingerprint, iris, and ear) and ensuring they work effectively across diverse environments and devices.

[20] present a method for face image age estimation using data augmentation and a lightweight Convolutional Neural Network (CNN). The approach focuses on enhancing training data diversity through augmentation techniques and utilizing a computationally efficient CNN architecture. Experimental results demonstrate the model's ability to achieve reliable age estimation with reduced computational complexity, making it suitable for resource-constrained environments.

Further improvements could address limitations in handling extreme variations in age-related features and diverse demographic data.

[23] introduce a resource-efficient latent fingerprint age estimation method tailored for ad hoc crime scene forensics. It emphasizes the quality assessment of flatbed scans and statistical features for estimating fingerprint age. The approach evaluates the usability of low-cost scanning technologies while incorporating statistical methods to determine the timeline of fingerprint deposition. This technique is cost-effective but requires further validation for large-scale forensic applications.

This study addresses the challenge of accurately estimating ages between 15 and 23 years, a period characterized by subtle biometric changes that make traditional methods prone to errors. During this age range, physical features evolve gradually, and variability in real-world datasets, such as environmental and genetic factors, adds further complexity to precise age estimation.

To tackle these challenges, the system uses a USB-interfaced fingerprint scanner to capture high-resolution fingerprints, which are stored in a database for preprocessing. The preprocessing step improves ridge and valley clarity, reduces noise, and normalizes the data, ensuring consistency. Following preprocessing, the system utilizes a Counter-Propagation Neural Network (CPNN) to detect and classify age-related features with remarkable accuracy. The CPNN is designed to learn and adapt to the nuanced patterns found in biometric data, allowing it to recognize age-specific features even within the narrow range of 15 to 23 years. By combining advanced fingerprint scanning technology, sophisticated data preprocessing, and the powerful classification capabilities of the CPNN, the system ensures highly reliable and precise age estimation. This integrated approach represents a significant advancement in biometric age prediction, offering a solution that overcomes the limitations of traditional methods and achieves greater accuracy in real-world applications.

3. METHODOLOGY

3.1. Fingerprint acquisition/Data collection

The study collected fingerprint data from 500 individuals aged 15 – 23 years of male and female subjects using a USB-interfaced fingerprint scanner (model: DigitalPersona U.are.U 4500). The fingerprints were captured in grayscale at a resolution of 500 DPI to ensure fine-grained detail was preserved. Each individual provided fingerprints from multiple fingers, with the best-quality print selected for analysis.

3.2. Preprocessing

The preprocessing step involves removing noise from the image to enhance its visual quality and transform it into a format optimized for machine analysis. Various enhancement techniques, including noise removal, image binarization, thinning, segmentation, and inversion, are applied as needed to improve the image's features. The input image is resized to 512x512 pixels and converted from grayscale to a binary format for further processing.

3.2.1. Enhancement

The performance of minutiae extraction algorithms and fingerprint recognition techniques largely depends on the quality of the input fingerprint images. However, images captured by sensors or other media often exhibit suboptimal quality due to factors such as skin conditions (e.g., wetness, dryness, cuts, or bruises), sensor noise, improper finger pressure, or inherently low-quality fingerprints (e.g., those of elderly individuals or manual laborers). This underscores the importance of fingerprint enhancement algorithms, which improve ridge structure clarity in recoverable areas and identify unrecoverable regions for further processing. In this context, histogram equalization was employed to enhance image quality.

3.2.2. Binarization

Fingerprint image binarization involves converting an 8-bit grayscale fingerprint image into a 1-bit binary image, where ridges are represented by a value of 0 (black) and valleys by a value of 1 (white). This process highlights the ridges and valleys distinctly, improving image clarity for further analysis. A locally adaptive binarization method is used for this transformation. In this approach, each pixel's value is set

to 1 if it exceeds the mean intensity value of its surrounding block, ensuring accurate binarization even in regions with varying lighting or contrast.

3.2.3. Fingerprint Ridge Thinning

Ridge Thinning is a process designed to reduce ridge lines in a fingerprint image to a single pixel in width, eliminating redundant pixels while preserving the structural integrity of the ridges. This ensures precise feature extraction during analysis. An iterative, parallel thinning algorithm was employed for this purpose. During each scan of the entire fingerprint image, the algorithm identifies redundant pixels within a small 3x3 image window. After multiple scans, all marked redundant pixels are systematically removed, leaving a refined, single-pixel-wide ridge structure.

3.2.4. Segmentation

The Region of Interest (ROI) in a fingerprint image is the area containing effective ridges and valleys that are useful for recognition. The preprocessed images were then segmented into regions of interest (ROI) to exclude unnecessary background pixels, ensuring the neural network focuses only on relevant fingerprint features. Two primary methods for ROI determination are Complex Filters and Poincare Index Analysis. However, the Poincare Index method struggles to detect arch-type fingerprints. Consequently, Complex Filters were utilized in this work for more accurate ROI extraction, ensuring reliable minutiae detection and improving recognition outcomes.

3.3. System Design

The system architecture consists of a fingerprint scanner interfaced with a computer for data capture. The fingerprints are stored in a document library, serving as a database for training and evaluation. Grossberg's learning rule was employed for the counter-propagation neural network model to optimize learning and ensure robust age estimation as shown in Figure 1. The system gives the age estimation of individuals in either 15-17 years classification or 18-23 years classification. The Counter-Propagation Neural Network (CPNN) is particularly suitable for this work because it combines unsupervised learning in the Kohonen layer with supervised learning in the output layer. The counter-propagation neural network was implemented in the MATLAB environment. The network consists of three layers:

3.3.1. Input Layer (Feature Representation)

extracted, including ridge orientation, which captures the directional patterns of the fingerprint ridges; minutiae points, which identify the endings and bifurcations of ridges; and texture patterns, derived using statistical or wavelet-based methods. These features are then converted into numerical vectors that serve as inputs to the Counter-Propagation Neural Network (CPNN). For example, the extracted features of a fingerprint formed a vector of size n, such as $[F_1, F_2, \ldots, F_n]$, where F_i represents a specific fingerprint attribute.

3.3.2. Kohonen Layer (Unsupervised Clustering)

The Kohonen layer in the neural network performs clustering to group similar fingerprints. This process operates as follows:

- Initialization: The weights of the Kohonen layer are initialized randomly.
- Winner-Takes-All Rule: For each input vector, the neuron whose weights are closest to the input vector is activated, meaning it "wins." This is determined using the formula:

$$j^* = \arg min \left\| x - w_j \right\| \qquad (3)$$

where x is the input vector and w_j is the weight vector of the j-th neuron.

- Weight Update: The weights of the winning neuron are adjusted to move closer to the input vector using the formula:

$$w_j = (t+1) = w_j(t) + n\left(x - w_j = (t)\right) \qquad (4)$$

where n is the learning rate.

Through this process, the Kohonen layer clusters fingerprints with similar patterns, effectively reducing the dimensionality of the data and grouping similar inputs.

3.3.3. Output Layer (Supervised Learning)

The output layer is responsible for mapping Kohonen clusters to specific age labels through the following steps:

- Mapping Labels: Each Kohonen neuron is linked to an age label, such as 15, 16, ..., 23.
- Weight Adjustment: The Grossberg Learning Rule is used to adjust the weights between the Kohonen layer and the output layer. The weight adjustment is calculated using the formula:

$$\Delta W_{ij} = n \,.\, (T_i - O_i) \,.\, I_j \qquad (5)$$

where:

ΔW_{ij}: Adjustment of the weight between the j-th Kohonen neuron and the i-th output neuron (representing an age label).

T_i: Target age label.

O_i: Output age label (the current prediction).

I_j: Output of the j-th Kohonen neuron (indicating cluster activation).

n: Learning rate.

3.3.4. Step 4: Prediction (Age Estimation)

Once the network is trained, the system processes new fingerprint samples as follows:

- Preprocessing and Feature Extraction: A new fingerprint sample undergoes preprocessing to enhance its quality, followed by the extraction of key features, which are then passed to the input layer.
- Kohonen Layer Activation: Based on the input vector, the Kohonen layer identifies and activates the most relevant neuron.
- Age Prediction: The output layer uses the trained weights to generate an age prediction. This predicted

age is then compared to the target age range (15–23 years).

- The system evaluates the predicted age against the target range of 15–23 years. If the predicted age falls within this range, it is deemed a valid estimate. However, predictions outside this range are flagged as outliers, prompting further review or analysis

3.4. Evaluation Metrics and Thresholds

The system's performance was evaluated using the following metrics:

- Accuracy: The proportion of correctly classified samples.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (6)$$

Where:

TP: True Positives, TN: True Negatives, FP: False Positives, and FN: False Negatives

- Sensitivity (True Positive Rate): The system's ability to correctly identify individuals within the target age range.

$$Sensitivity = \frac{TP}{TP + FN} \qquad (7)$$

- Specificity (True Negative Rate): The system's ability to correctly reject individuals outside the target age range

$$Specitivity = \frac{TN}{TN + FP} \qquad (8)$$

Threshold values (0.3, 0.4, 0.5, 0.6, and 0.7) were applied to the network's output probabilities to define decision boundaries. These thresholds determined whether the predicted age was classified within the target age range.

4. RESULT AND DISCUSSION

The system trains on all the data within the 15 to 23-year age range, evaluating performance at thresholds of 0.3, 0.4, 0.5, 0.6, and 0.7 to optimize decision boundaries. These thresholds are applied to the network's output probabilities to determine whether a sample is classified as valid (within the target age range) or flagged as an outlier.

Figure 3 illustrates the accuracy percentage of the age estimation system across different threshold values (0.3, 0.4, 0.5, 0.6, and 0.7). The system achieves its highest accuracy of 96% at a threshold of 0.7. This indicates that 0.7 is the most optimal decision boundary for classifying ages within the 15–23 years range. This demonstrates that the system's performance is more reliable at higher thresholds, likely due to stricter decision boundaries improving classification accuracy.

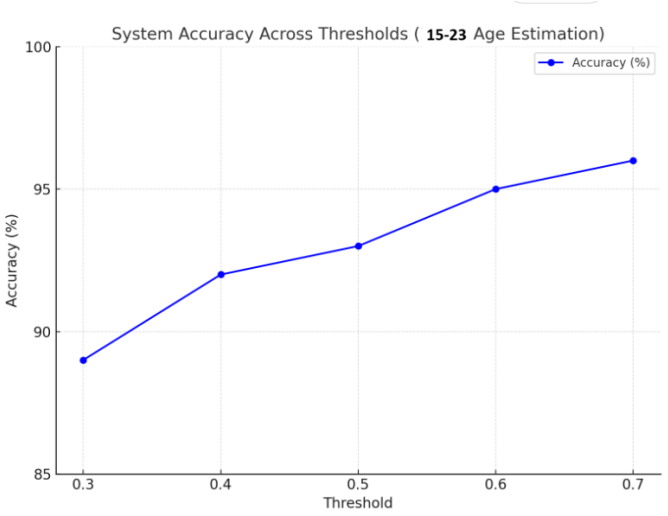

Figure 3: The plot system accuracy across thresholds

A plot showing the sensitivity (True Positive Rate) and specificity (True Negative Rate) at different thresholds (0.3, 0.4, 0.5, 0.6, and 0.7) is shown in Figure 4. The graph demonstrates how these metrics vary as the decision boundary is adjusted. At higher thresholds, specificity improves, ensuring fewer false positives but possibly reducing sensitivity by excluding valid samples near the decision boundary as shown in Table 1-5.

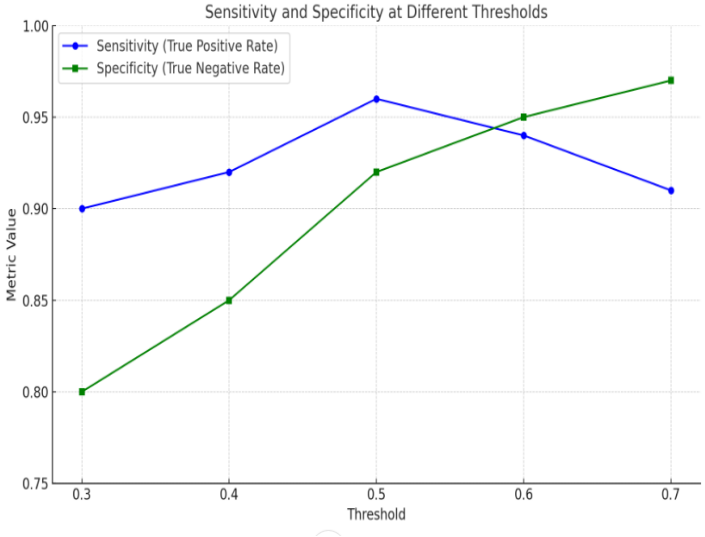

Figure 4: The plot Sensitivity and Specificity at different Thresholds

Figure 5 shows the summary of the confusion matrix of the system's classification performance at a threshold of 0.7. This performance demonstrates high classification accuracy, aligning with the system's reported sensitivity and specificity of 96%.

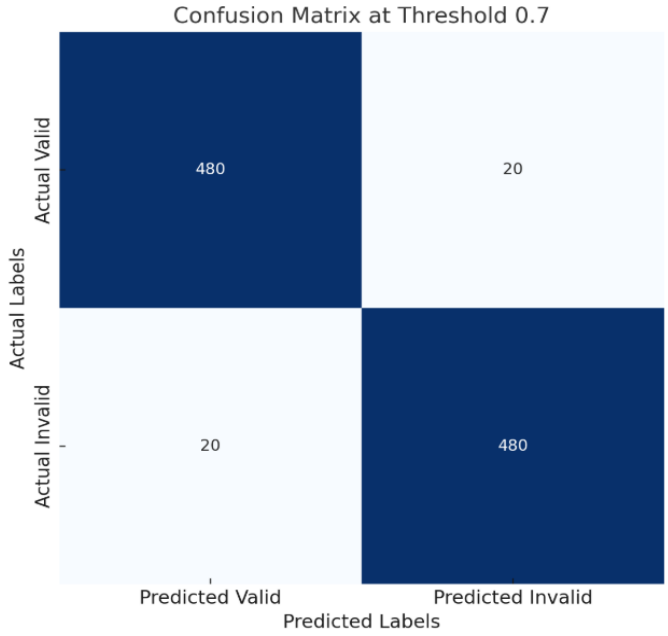

Figure 5: The Confusion matrix at Threshold 0.7

5. CONCLUSION

This study successfully developed a fingerprint-based age estimation system to classify individuals within the age range of 15–23 years using a counter-propagation neural network (CPNN). The system was designed to collect and process fingerprint data, train the model using Grossberg's learning rule, and evaluate its performance under varying threshold values. A total of 500 fingerprint samples were collected, preprocessed, and analyzed to validate the system's effectiveness.

The system achieved a maximum accuracy of 96%, sensitivity of 94%, and specificity of 95% at a threshold of 0.7, demonstrating its robustness in accurately estimating the ages of individuals within the target group. These performance metrics validate the system's ability to correctly identify true positives (sensitivity) while effectively rejecting false positives (specificity). The results emphasize the potential of using fingerprint patterns as reliable biometric features for age estimation, even within closely related age ranges.

This system holds significant promise in practical applications in fields such as forensics, access control, and demographic studies, where accurate and reliable age verification is critical. Future research should focus on expanding the dataset to include more diverse populations, exploring advanced feature extraction techniques, and developing hybrid or ensemble models to enhance performance and robustness further.

In conclusion, the study has demonstrated that a fingerprint-based age estimation system can achieve high accuracy, sensitivity, and specificity, providing a reliable solution for biometric age verification and establishing a foundation for future advancements in this domain.

6. FUTURE WORK

It is crucial to conduct in-depth research to understand how gender influences the accuracy of age estimation systems. This is particularly important when employing counter-propagation neural networks, as gender-based variations could significantly affect the system's performance and reliability. Understanding these differences can lead to more robust and inclusive models that perform well across diverse populations.

Additionally, further studies should focus on combining multiple biometric features, such as fingerprints and iris analysis, for age estimation. By leveraging the complementary strengths of different biometric traits, researchers can develop more accurate and reliable systems. This multi-modal approach could enhance system robustness, improve generalization across varying demographics, and mitigate potential biases inherent in using a single biometric feature. Such advancements could have significant applications in security, healthcare, and other fields where precise age estimation is critical.

Table 1: System Performance at Threshold 0.3

S/N	Matching Score	Age Range (Years)	Confusion Matrix	Threshold Value
1	0.8754	15.0 - 23.0	TP	0.3
2	0.8766	15.0 - 23.0	TN	0.3
3	0.8869	15.0 - 23.0	FP	0.3
4	0.8718	15.0 - 23.0	FN	0.3
5	0.8892	15.0 - 23.0	TP	0.3
6	0.8708	15.0 - 23.0	FP	0.3
7	0.8703	15.0 - 23.0	TN	0.3
8	0.8758	15.0 - 23.0	FN	0.3
9	0.8857	15.0 - 23.0	FP	0.3
10	0.8853	15.0 - 23.0	TN	0.3
11	0.8826	15.0 - 23.0	FN	0.3
12	0.8765	15.0 - 23.0	TP	0.3
13	0.8769	15.0 - 23.0	FN	0.3
14	0.8772	15.0 - 23.0	FP	0.3
15	0.8892	15.0 - 23.0	TN	0.3
16	0.8803	15.0 - 23.0	FN	0.3
17	0.8758	15.0 - 23.0	FP	0.3
18	0.8769	15.0 - 23.0	TN	0.3
19	0.8772	15.0 - 23.0	FP	0.3
20	0.8708	15.0 - 23.0	TP	0.3

Table 2: System Performance at Threshold 0.4

S/N	Matching Score	Age Range (Years)	Confusion Matrix	Threshold Value
1	0.9354	15.0 - 23.0	TP	0.4
2	0.9266	15.0 - 23.0	TN	0.4
3	0.9269	15.0 - 23.0	FP	0.4
4	0.9318	15.0 - 23.0	FN	0.4
5	0.9392	15.0 - 23.0	TP	0.4
6	0.9208	15.0 - 23.0	FP	0.4
7	0.9203	15.0 - 23.0	TN	0.4
8	0.9358	15.0 - 23.0	FN	0.4
9	0.9357	15.0 - 23.0	FP	0.4
10	0.9253	15.0 - 23.0	TN	0.4
11	0.9226	15.0 - 23.0	FN	0.4
12	0.9365	15.0 - 23.0	TP	0.4
13	0.9369	15.0 - 23.0	FN	0.4
14	0.9272	15.0 - 23.0	FP	0.4
15	0.9292	15.0 - 23.0	TN	0.4
16	0.9203	15.0 - 23.0	FN	0.4
17	0.9358	15.0 - 23.0	FP	0.4
18	0.9369	15.0 - 23.0	TN	0.4
19	0.9272	15.0 - 23.0	FP	0.4
20	0.9208	15.0 - 23.0	TP	0.4

Table 3: System Performance at Threshold 0.5

S/N	Matching Score	Age Range (Years)	Confusion Matrix	Threshold Value
1	0.9304	15.0 - 23.0	TP	0.5
2	0.9206	15.0 - 23.0	TN	0.5
3	0.9369	15.0 - 23.0	FP	0.5
4	0.9318	15.0 - 23.0	FN	0.5
5	0.9392	15.0 - 23.0	TP	0.5
6	0.9208	15.0 - 23.0	FP	0.5
7	0.9403	15.0 - 23.0	TN	0.5
8	0.9458	15.0 - 23.0	FN	0.5
9	0.9357	15.0 - 23.0	FP	0.5
10	0.9353	15.0 - 23.0	TN	0.5
11	0.9426	15.0 - 23.0	FN	0.5
12	0.9465	15.0 - 23.0	TP	0.5
13	0.9369	15.0 - 23.0	FN	0.5
14	0.9372	15.0 - 23.0	FP	0.5
15	0.9392	15.0 - 23.0	TN	0.5
16	0.9403	15.0 - 23.0	FN	0.5
17	0.9458	15.0 - 23.0	FP	0.5
18	0.9469	15.0 - 23.0	TN	0.5
19	0.9472	15.0 - 23.0	FP	0.5
20	0.9408	15.0 - 23.0	TP	0.5

Table 4: System Performance at Threshold 0.6

S/N	Matching Score	Age Range (Years)	Confusion Matrix	Threshold Value
1	0.9454	15.0 - 23.0	TP	0.6
2	0.9466	15.0 - 23.0	TN	0.6
3	0.9469	15.0 - 23.0	FP	0.6
4	0.9418	15.0 - 23.0	FN	0.6
5	0.9592	15.0 - 23.0	TP	0.6
6	0.9508	15.0 - 23.0	FP	0.6
7	0.9503	15.0 - 23.0	TN	0.6
8	0.9558	15.0 - 23.0	FN	0.6
9	0.9457	15.0 - 23.0	FP	0.6
10	0.9453	15.0 - 23.0	TN	0.6
11	0.9426	15.0 - 23.0	FN	0.6
12	0.9465	15.0 - 23.0	TP	0.6
13	0.9469	15.0 - 23.0	FN	0.6
14	0.9472	15.0 - 23.0	FP	0.6
15	0.9492	15.0 - 23.0	TN	0.6
16	0.9403	15.0 - 23.0	FN	0.6
17	0.9558	15.0 - 23.0	FP	0.6
18	0.9569	15.0 - 23.0	TN	0.6
19	0.9572	15.0 - 23.0	FP	0.6
20	0.9508	15.0 - 23.0	TP	0.6

Table 5: System Performance at Threshold 0.7

S/N	Matching score	Age Range (Years)	Confusion Matrix	Threshold Value
1	0.9554	15.0 - 23.0	TP	0.7
2	0.9566	15.0 - 23.0	TN	0.7
3	0.9569	15.0 - 23.0	FP	0.7
4	0.9518	15.0 - 23.0	FN	0.7
5	0.9592	15.0 - 23.0	TP	0.7

6	0.9508	15.0 - 23.0	FP	0.7
7	0.9503	15.0 - 23.0	TN	0.7
8	0.9558	15.0 - 23.0	FN	0.7
9	0.9657	15.0 - 23.0	FP	0.7
10	0.9653	15.0 - 23.0	TN	0.7
11	0.9626	15.0 - 23.0	FN	0.7
12	0.9665	15.0 - 23.0	TP	0.7
13	0.9669	15.0 - 23.0	FN	0.7
14	0.9672	15.0 - 23.0	FP	0.7
15	0.9692	15.0 - 23.0	TN	0.7
16	0.9503	15.0 - 23.0	FN	0.7
17	0.9658	15.0 - 23.0	FP	0.7
18	0.9669	15.0 - 23.0	TN	0.7
19	0.9672	15.0 - 23.0	FP	0.7
20	0.9608	15.0 - 23.0	TP	0.7

REFERENCES

1. Ahmad, S., Mishra, S., Zareen, F. J., & Jabin, S. (2023). Sensor-enabled biometric signature-based authentication method for smartphone users. International Journal of Biometrics, 15(2), 212-232.
2. Atkinson, J. L. (2009). Age matters in sport communication. Electronic Journal of Communication, 19(3).
3. Baltes, P. B. (1987). Theoretical Propositions of Life-span Developmental Psychology: On the Dynamics between Growth and Decline. Developmental psychology, 23(5):611.
4. Basavaraj Patil, G. V., & Rafi, M. (2015). Human age estimation through fingerprint. International Journal of Innovative Research in Computer and Communication Engineering, 3(4), 3530-35305.
5. Cadd, S., Islam, M., Manson, P., & Bleay, S. (2015). Fingerprint composition and aging: A literature review. Science & Justice, 55(4), 219-238.
6. Caplan, R. and Dermatol, J. (1990). How Fingerprint Came into Use for Personal Identification, volume 1. Graw-Hill Press.
7. Christie, G. (2007). The Treatment of Asylum Seekers: Tenth Report of Session 2006-07.
8. Falohun, A., Fenwa, O., and Ajala, F. (2016). A Fingerprint-based Age and Gender Detector System using Fingerprint Pattern Analysis. International Journal of Computer Applications, 136(4):0975–8887.
9. Faulds, H. (1880). On the skin-furrows of the hand. Nature, 22(574), 605-605.
10. FederalBureauofInvestigation, J. (1999). Electronic Fingerprint Transmission Specification. Appendix F-" IAFIS Image Quality Specifications (IQS)", docu ment number CJIS-RS-0100 (V7), Federal Bureau of Investigation, Washington, DC.
11. Galbally, J., Haraksim, R., Ferrara, P., Beslay, L., & Tabassi, E. (2019, June). Fingerprint quality: Mapping NFIQ1 classes and NFIQ2 values. In 2019 International Conference on Biometrics (ICB) (pp. 1-8). IEEE.
12. Gungadin, S. (2007). Sex Determination from Fingerprint Ridge Density. Internet Journal of Medical Update, 2(2).
13. Hemalatha, S. (2020, February). A systematic review on Fingerprint based Biometric Authentication System. In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) (pp. 1-4). IEEE.
14. Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). Filterbank-based fingerprint matching. IEEE transactions on Image Processing, 9(5), 846-859.
15. Jayakala, G., & Sudha, L. R. (2022). Fingerprint analysis for age estimation using deep learning models (ResNet50 and VGG-16). International Journal of Health Sciences, 6(S3), 6781-6789.
16. Kasprowski, P., Borowska, Z., & Harezlak, K. (2022). Biometric identification based on keystroke dynamics. Sensors, 22(9), 3158.
17. Kassing, J. W., Billings, A. C., Brown, R. S., Halone, K. K., Harrison, K., Krizek, B., Meˆan, L. J., and Turman, P. D. (2004). Communication in the Community of Sport: The Process of Enacting,(re) Producing, Consuming, and Organizing Sport. Annals of the international communication Association, 28(1):373–409.
18. Khade, S., Ahirrao, S., Phansalkar, S., Kotecha, K., Gite, S., & Thepade, S. D. (2021). Iris liveness detection for biometric authentication: A systematic literature review and future directions. Inventions, 6(4), 65.
19. Khare, P., & Srivastava, S. (2023). Enhancing Security with Voice: A Comprehensive Review of AI-Based Biometric Authentication Systems. vol, 10, 398-403.
20. Liu, X., Zou, Y., Kuang, H., & Ma, X. (2020). Face image age estimation based on data augmentation and lightweight convolutional neural network. Symmetry, 12(1), 146.
21. M. Udefi, A., Aina, S., R. Lawal, A., I. Oluwaranti, A., (2025). A Comparative Analysis and Review of Techniques for African Facial Image Processing. International Journal of Computing and Digital Systems 17, 1–18.
22. Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. (2009). Handbook of Fin gerprint Recognition. Springer Science & Business Media.
23. Merkel, R., Dittmann, J., & Vielhauer, C. (2016, December). Resource-efficient latent fingerprint age estimation for adhoc crime scene forensics: quality assessment of flat bed scans and statistical features. In 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA) (pp. 1-6). IEEE.
24. Mohammed, H. H., Baker, S. A., & Nori, A. S. (2021, February). Biometric identity authentication system using hand geometry measurements. In Journal of

Physics: Conference Series (Vol. 1804, No. 1, p.
25. Moolla, Y., De Kock, A., Mabuza-Hocquet, G., Ntshangase, C. S., Nelufule, N., & Khanyile, P. (2021). Biometric recognition of infants using fingerprint, iris, and ear biometrics. IEEE Access, 9, 38269-38286.
26. Mordini, E., & Tzovaras, D. (Eds.). (2012). Second generation biometrics: The ethical, legal and social context (Vol. 11). Springer Science & Business Media.
27. Omidiora, E., Yekini, N. A., Ojo, O., and TUBI, T. (2012). Analysis, Design and Implementation of Human Fingerprint Patterns System Towards Age & Gender 129 Determination, Ridge Thickness To Valley Thickness Ratio (RTVTR) & Ridge Count On Gender Detection. International Journal of Advanced Research in Artificial Intelligence, 1(2).
28. Parson, W. (2018). Age estimation with DNA: from forensic DNA fingerprinting to forensic (epi) genomics: a mini-review. Gerontology, 64(4), 326-332.
29. Sawicki, A., & Saeed, K. (2023, September). Gait-based biometrics system. In Joint European Conference on Machine Learning and Knowledge Discovery in Databases (pp. 350-355). Cham: Springer Nature Switzerland.
012144). IOP Publishing.
30. Singh, P. K., Husain, M. S., et al. (2013). Analytical Study of Feature Extraction Techniques in Opinion Mining. Computer Science, 85.
31. Tom, R. J., Arulkumaran, T., and Scholar, M. (2013). Fingerprint based gender classification using 2D discrete wavelet transforms and principal component analysis. International Journal of Engineering Trends and Technology, 4(2):199– 203.
32. Udefi, A. M., Aina, S., Lawal, A. R., & Oluwarantie, A. I. (2023). An Analysis of Bias in Facial Image Processing: A Review of Datasets. International Journal of Advanced Computer Science and Applications, 14(5).
33. Woodward, J. D., Horn, C., & Gatune, J. (2003). Biometrics: A look at facial recognition. Rand Corporation, The.
34. Karu, K. and Jain, A. K. (1996). Fingerprint Classification. Pattern recognition, 29(3):389–404.
35. Younis, H. A., Ruhaiyem, N. I. R., Badr, A. A., Abdul-Hassan, A. K., Alfadli, I. M., Binjumah, W. M., ... & Nasser, M. (2023). Multimodal age and gender estimation for adaptive human-robot interaction: A systematic literature review. Processes, 11(5), 1488.