SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I8P126

Volume 12 Issue 8, 293-306, August 2025
© 2025 Seventh Sense Research Group®

Original Article

Security for Distributed Deep Neural Networks in Miniature Fingerprint Recognition Utilizing a Genetic Algorithm

S. Anantha Babu[1], S. Gnana Selvan[2], C. Mahesh[3], R. Jeena[4], S. Jagadeesh[5], S. Samsudeen Shaffi[6]

[1]Department of Computer Science and Engineering, GITAM School of Technology, GITAM University, Bangalore, India.
[2]Department of Electronics and Communication Engineering, Jayaraj Annapackiam CSI College of Engineering, Nazareth, Chennai, India.
[3]Department of Computer Science and Engineering, Emerging Technologies, SRM Institute of Science and Technology, Vadapalani Campus, India.
[4]Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, India.
[5,6]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India.

[5]Corresponding Author : jagadeesh15.sj@gmail.com

Received: 14 June 2025 Revised: 15 July 2025 Accepted: 16 August 2025 Published: 30 August 2025

Abstract *- The most traditional and popular biometric identification method is based on fingerprints. Everybody has a set of unchanging, distinctive fingerprints. It is essential to label minutiae appropriately and reject fake ones since recognition systems rely on local ridge characteristics. As a result, fingerprint pictures need to be controlled for clarity, minute results need to be computed, and then templates need to be compared to templates that are kept in the database. The research suggested three methods to enhance images, extract information, and match with fingerprint templates. The study's first phase included 300 x 300 neural network picture inputs with various fingerprints gathered from two sets of false and actual images. In order to anticipate the optimal miniature extraction using genetically based chromosomal matching miniature analysis, we then use the VGG16 model. The suggested Model predicts 96.20 for smaller datasets, and when the size of the dataset was enlarged, the accuracy decreased to 86.89 percent, which may be employed in practical applications and contributes to system security.*

Keywords *- VGG16, AlexNet, ResNet, Genetic Algorithm, Finger Print Classification.*

1. Introduction

Learning necessitates the fundamental cognitive capacity to identify and distinguish among diverse items or patterns. This process commences with the collection of sensory input and concludes with the integration of new information into current knowledge. In the domains of artificial intelligence and computer vision, machine vision seeks to emulate human abilities by allowing computers to recognize and analyze things in real-world settings. Despite considerable advancements, the identification of three-dimensional objects under varying ambient circumstances remains a substantial difficulty. A significant sector in which machine vision has shown substantial success is biometrics, especially in fingerprint identification. Fingerprint identification systems rely significantly on feature extraction methods, which provide the basis for matching algorithms [1, 2].

Raw biometric pictures often exhibit noise and poor contrast, requiring preprocessing procedures like segmentation, augmentation, orientation estimation, binarization, and thinning.

In the identification phase, a 1:N matching method is used to identify probable matches in a database of fingerprint templates, while acceleration methods are implemented to minimize the search area and enhance processing efficiency [3]. Biometrics is the scientific study of using biological characteristics, including fingerprints, iris patterns, palm prints, face scans, DNA, and voiceprints, for individual identification [4]. Fingerprints are extremely distinctive, even among identical twins, making them very helpful in global forensic investigations. The extensive use of fingerprint-based identification has led to the creation of large databases, requiring efficient and precise recognition systems [5].

Several methods achieve fingerprint detection, including ultrasonic, optical, and capacitive sensors. Each sensor type functions based on unique physical principles: ultrasonic sensors use reflected sound waves, optical sensors acquire light-based pictures, and capacitive sensors identify fluctuations in electrical fields due to changes in surface topography [6]. The disparities in sensing systems often result in discrepancies in collected fingerprint characteristics, which complicates the process of universal identification [7]. The primary characteristics collected for fingerprint identification generally include ridge flow, ridge frequency, terminations, and core/delta points. However, both external and internal variables, such as finger pressure, skin condition, distortion, and image alignment, significantly influence performance [8].

Furthermore, current identification methods often depend on incomplete fingerprint scans, which limits precision. To mitigate this constraint, there is a growing exploration of models capable of reconstructing whole fingerprint imprints [9, 10]. This study enhances existing research by presenting a fingerprint identification system that combines Convolutional Neural Networks (CNNs) with genetic algorithms. Convolutional Neural Networks (CNNs) have the ability to learn hierarchical features from unprocessed fingerprint photos, differentiating nuanced variations across patterns.

The proposed research presents an innovative hybrid architecture that combines a distributed deep neural network with a Genetic Algorithm (GA)-based feature optimization for tiny fingerprint identification. In contrast to traditional CNN-based biometric models that utilize static, high-dimensional feature maps, this method employs VGG16 to extract hierarchical fingerprint representations and GA to dynamically select the most discriminative features for low-resolution, partial inputs produced by miniature sensors. This dual-layer solution tackles significant issues in cross-sensor generalization, dataset heterogeneity, and resource-limited deployment by reducing feature redundancy and enhancing model adaptability across distributed infrastructures. Moreover, the GA-based feature subset functions as both an accuracy booster and a lightweight encryption layer for safe feature transmission, offering a comprehensive solution to the security and efficiency deficiencies in remote fingerprint recognition systems.

Our Model presents a distributed deep neural network for tiny fingerprint identification, augmented by a feature optimization layer based on a Genetic Algorithm (GA). In contrast to traditional CNN designs that depend on static feature maps, the GA dynamically identifies the best discriminative VGG16 features, considerably diminishing redundancy and enhancing generalization across low-resolution and cross-sensor datasets. Experimental findings on the FCV2000, FCV2002, and FCV2004 datasets indicate that the suggested Model attains an EER ranging from 1.0% to 2.4%, in contrast to the 6% to 9% observed in VGG16, AlexNet, ResNet, and conventional CNN methodologies. This illustrates a significant progression beyond current research by offering a lightweight, secure, and highly accurate fingerprint recognition framework tailored for distributed biometric systems.

The next sections of this article are organized as follows: Section 2 provides a background study, examining current fingerprint identification techniques, sensor technologies, and the constraints of conventional methods. Section 3 delineates the proposed methodology, including the VGG16-based architecture, preprocessing methodologies, and optimization approaches used to augment accuracy and efficiency. Section 4 delineates the performance assessment, including the experimental configuration, dataset utilization, evaluation criteria, and a comparison with baseline methodologies. Section 5 closes the research and addresses prospective improvements, including the integration of multimodal biometrics, real-time deployment tactics, and adaptive learning mechanisms to promote system generalizability.

2. Related Work

Deep learning methods have evolved a lot in the last 30 years. The advancements made in this area have profoundly affected several software packages using computer vision and pattern recognition. Since improving identification accuracy is a high priority, automated fingerprint recognition is a rapidly growing area of study. In addition, deep learning techniques eliminate the importance of manually extracted characteristics in favour of a broader approach to analysis. In this part, we look at some of the most recent studies that have focused on how best to catalogue fingerprint images.

This technique has been proposed for applications like access control, ATM user verification, and criminal identification using a fingerprint data collection. In the author's analyses forged fingerprints come to the conclusion that current fingerprint verification systems cannot effectively spot forgeries. It has been determined that adjusting the fingerprints has no effect on the picture quality. An effective method for identifying a forged fingerprint is now available. Significant advances in deep learning techniques have been made during the last three decades. These innovations greatly influenced several software packages using computer vision and pattern recognition [12-14].

Due to the need for high identification rates, research into automated fingerprint recognition is a hot issue. Furthermore, deep learning techniques move the emphasis away from approaches dedicated to detail extraction as handcrafted features and instead concentrate on the analysis of the whole picture. The most recent studies on the subject of fingerprint image classification are discussed. In order to extract features based on minute differences, preprocessed contactless fingerprints must have their RGB pictures transformed to grayscale. Thus, machine learning must also be used for ROI, including tasks like ridge valley extraction and finger orientation prediction for the smallest details. In order to extract the ROI after finger detection, width, height, and resolution must be normalized. The input to this preliminary 3D contactless fingerprint processing step is an image of the fingerprint extraction.

Finger detection and ROI extraction are both performed after the fact in the output. Contactless 3D finger geometry is essential for the colour-based segmentation of ROI extraction-limited setups. Several processes relied on the ridge's form and direction to identify its centre. A Support Vector Machine (SVM) can quickly and accurately categorise fingerprints based on their minute details, with those details themselves serving as detection points. The grey mean, grey variance, contrast, coherence, and main energy ratio are five feature vector lengths that SVM may use to evaluate an image's quality. The training required to integrate these features is extensive [15-17].

Employing an innovative method grounded on chaos theory and Hadamard matrices, Fingerprint and Iris Template Protection for Health Information System Access and Security tackles the problem of template database breaches, including threats to the integrity of biometric templates. Despite the extensive research on safeguarding biometric templates, the majority of the methods presented in the literature fall short of meeting the primary criteria of safety, efficiency, variety, and revocability. However, our method not only satisfies the needs of revocability, diversity, and privacy but also provides superior results in the cases of recognition rate (i.e., one hundred percent), false rejection rate (zero percent), and false acceptance rate (one hundred percent). This allows us to detect low-rate attacks with greater accuracy [18].

NLP, speech recognition, and object identification are just a few of the areas where deep learning has shown promising results. It also has remarkable results in biometrics, namely with a finger vein recognition system. The research uses Alex Net and VGG 16 architectures to improve upon previous methods of finger vein identification. To address the issue of low-quality images and insufficient data, the FV-GAN model is presented as a Generative Adversarial Network (GAN) Model for finger vein, based on the Cycle-GAN architecture. The authors present a fully convolutional neural network, an extension of U-Net, integrated with a conditional random field as an end-to-end system for pixel-wise fingerprint datasets to enhance vein pattern segmentation. This approach improves upon prior methods by modifying the Densenet-161 architecture and incorporating a distinctive embedding module into the core model [19-21]. There was some encouraging data from experiments using deep learning algorithms for finger vein detection. Unfortunately, inadequate data is still a challenge for the available approaches.

The suggested approach differs from Current Genetic Algorithm (GA)-based fingerprint classification studies in that it presents many distinctive additions. This research integrates GA-driven optimization with deep hierarchical features extracted from VGG16, facilitating adaptive feature selection in high-dimensional CNN representations in contrast to traditional GA methods that rely on handcrafted or minutia-based descriptors in centralized architectures.

The framework is specifically tailored for miniature fingerprint sensors and low-resolution data, a context seldom explored in previous GA-based research, and additionally integrates a distributed deep neural network architecture with secure feature transmission to facilitate privacy-preserving biometric processing. By dynamically eliminating superfluous activations and concentrating on distinguishing patterns, the Model attains computational efficiency and improved generalization across diverse and cross-sensor datasets. This integration of deep feature learning, genetic algorithm optimization, and distributed security signifies a significant progression beyond previous genetic algorithm-based fingerprint classification studies, positioning the proposed system as a scalable and high-performance option for next-generation biometric authentication.

The deficiencies underscore the need for a secure, distributed, deep neural network architecture that dynamically optimises deep hierarchical features for tiny fingerprint detection. A hybrid methodology integrating VGG16-based deep learning with GA-driven feature selection minimizes duplication, improves cross-sensor flexibility, and achieves high accuracy in low-resolution scenarios while safeguarding biometric data transfer. Rectifying these deficiencies is essential for the advancement of scalable, privacy-preserving fingerprint recognition systems appropriate for next-generation IoT and mobile authentication contexts.

3. The Proposed Miniature-Based VGG16 Fingerprint Matching

3.1. Proposed Architecture

Figure 1 depicts the operational flow of the enhanced fingerprint matching architecture, including a Genetic Algorithm (GA). The procedure emphasizes critical phases like preprocessing, feature extraction using VGG16, and enhanced matching precision through GA-based optimization.

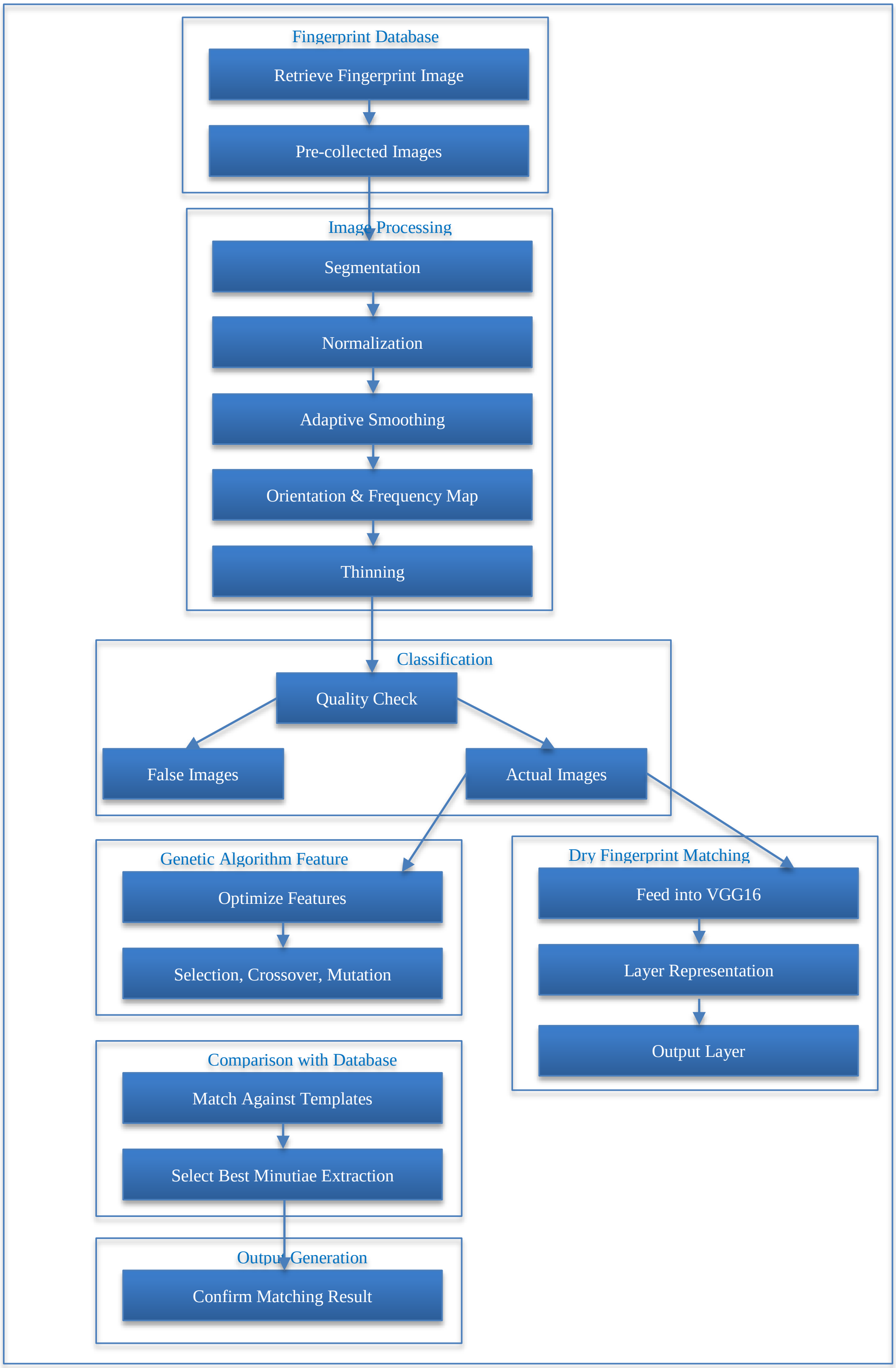

Fig. 1 Optimized fingerprint matching architecture with GA

Figure 1 represents the fingerprint identification process, which begins with the extraction of images from an existing database intended for training and testing. This is followed by segmentation to define the fingerprint area and normalization to standardize intensity values for a consistent contrast. Adaptive smoothing is applied to eliminate noise while preserving ridge structures. Subsequently, orientation and frequency mapping are conducted to optimize ridge flow, after which thinning produces a single-pixel skeleton for minutia extraction. A classification node identifies low-quality images and directs them to a Genetic Algorithm (GA)-based optimization pathway, while valid images progress to a VGG16-based deep learning pipeline.

This pipeline processes the fingerprints through sequential convolutional blocks (from Conv1_1 to Conv5_3, including pooling) and fully connected layers to extract hierarchical features. These features are refined using a genetic algorithm that employs selection, crossover, and mutation to retain only the most distinctive patterns. The optimized vector is then compared with stored database templates to identify the minutiae match with the highest similarity score. Ultimately, this process produces an output that verifies whether the input fingerprint matches a recorded template, ensuring robust and precise recognition.

3.2. Preprocessing

During the process of acquiring a fingerprint image, a lot of redundant data is collected. Scarred images, dry or damp fingertips and improper pressure are just a few of the issues that must be resolved in order to get a usable and accurate result. Thus, preprocessing of the new fingerprint images is required.

Fingerprint images may be preprocessed using enhancement, normalization, filtering, noise reduction, binarization, and thinning techniques. Binarization and thinning are used in this study, since they are prerequisite processes for fingerprint categorization and matching. The suggested architecture's preprocessing is divided into three stages: converting from 2D grayscale to 3D colour, binarization, and thinning [22].

3.2.1. Segmentation

Block-wise coherence is used to generate a mask to separate the ridges from the background and define the ROI. The variance is determined for each sub-block of (W W) size that is created in the image. It adopts the morphological operations "OPEN" and "CLOSE." Images can be expanded and background noise-induced peaks removed using the "OPEN" procedure. Images can be reduced in size, and tiny voids can be removed with the 'CLOSE' technique [23].

3.2.2. Image Normalization

An image's intensity can be improved by normalization, which involves altering the range of grey level values to bring them into a desirable range. During normalization, the grey level value along the ridges is standardized to make further processing more manageable. Each block undergoes normalization independently using the procedures outlined below. Instances of observation were counted in terms of their height and width. The total number of image widths divided by the total number of image heights gives the aspect ratio [23].

3.2.3. Adaptive Smoothening

After the background has been removed, a fingerprint is produced and adaptively smoothed with the help of local orientations. This method eliminates most minor defects. The local ridge orientation is used to achieve a uniform smoothing, whereas a Gaussian smoothing is used in the opposite direction.

The smoothing filter's kernel is the product of μ = 0 and σ= 1 normalized 5 x I uniform kernel with a 1 x 3 Gaussian kernel. There are 16 discrete options for the smoothing filter's orientation. Each pixel's orientation must be taken into account before a filter is applied to it. Being able to identify items is crucial in everyday life. To identify anything, one must go through a process of seeing it and linking it to previously stored knowledge. Robotic eyeballs identify patterns. Computer systems are being developed by scientists and engineers to recognize items in the real world. Nevertheless, despite considerable progress, there have been encouraging findings from studies conducted in sub-fields of this science, such as biometrics [24, 25].

3.2.4. Orientation Field

Sobel filters were employed to determine the direction of the field. The 3 by 3 operators Gx and Gy are employed to calculate the gradients in the horizontal and vertical directions.

3.2.5. Frequency Map

In computing a frequency block for constructing the Gabor filter, obtaining the local estimate of the frequency map in conjunction with the directional map is necessary.

3.2.6. Thinning

To simplify the extraction of details, the image must be "skeletonized" by removing unnecessary pixels from ridges until they are just one pixel wide.

3.2.7. Minutiae Extraction

To find ridge endpoints and ridge bifurcations, use the crossing number approach [26]. In 3x3 pixel blocks, the crossing number algorithm will operate. The CN value is calculated using the following formula.

$$CN(P) = \frac{1}{2}\sum_{i=1}^{8} |P_i - P_{i-1}|$$

3.2.8. Singularities

For closed curves, the Poincaré index assumes one of the discrete values: 0°, 180°, or 360°. This is well known and simple to demonstrate. Regarding singularities in fingerprints [27]:

- 0° is not associated with any specific area.
- 360° is classified as a unique area of the whorl type
- 180° is classified as a loop-type singular area
- 180° is classified as a delta-type unique area.

$$P_{G,C}(i,j) = \sum_{k=0,\ldots,7} angle(d_k, d_{(k+1) mod\ 8})$$

$$P_{G,C}(i,j) = \textstyle\sum_{k=0,\ldots,7}\ angle(d_k, d_{(k+1) mod\ 8} \qquad (2)$$

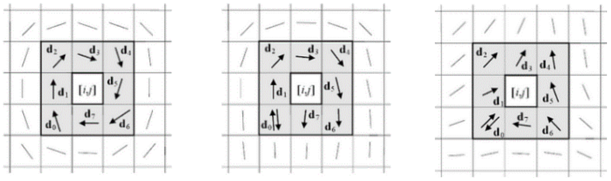

Fig. 2 Singularites search between 360°, 180° and -180°

3.3. Finger Print Matching Problem

Consider the sets of minutiae in the template and the query fingerprints are {(Xn1, Xn, 2)} and {(ym 1, ym 2)} respectively, where n = 1, 2, 3,..., N, and m = 1, 2, 3,..., M. The template fingerprints contain N and M, respectively, minutiae. The transformation between Xi and Y is Yj = F(Xi).

$$Yi = s.R.Xi + T$$

Finding the optimized transformation that can translate as many details from the template fingerprint to the query fingerprint as possible may be considered the solution to the matching issue [28].

3.3.1. Selecting Optimized Fingerprint Matching Technique

For the evaluation of their suitability for fingerprint identification, we have examined a wide range of frequently used optimization approaches [29].

1) This heuristic amalgamates a random walk with breadth-first search in the following manner.

- To get a relatively even distribution of states across the state graph, the sink node starts the whole process by doing a BFS of a user-specified depth, B, starting with the start states.
- The following is carried out concurrently by each processor i that gets a portion of the BFS frontier Qi. The number, N, of random walk steps for each processor would have been selected by the user (before the entire process starts). As a result, processor i performs N/q random walks on each of Qi's q states. Each random walk starts in a unique state in Qi, and every Sth state of each random walk is relayed to its home node. The probable secondary BFS start states are as follows,

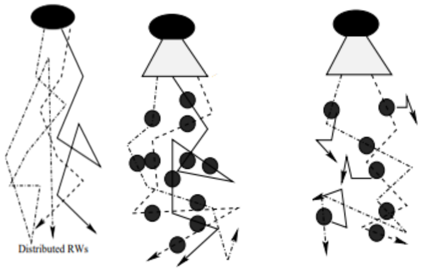

Fig. 3 Heuristic searches 1, 2, and 3 integrate distributed random walks with breadth-first search, whereas Heuristic 4 is a specific instance of Heuristic 3, characterized by a secondary breadth-first search depth of zero

- Employing calculus-based strategies (gradient approaches, resolving equation systems): The goal function does not have a mathematical closed-form formulation. The objective functional analysis reveals discontinuities and multimodal complexity.

3.3.2. Theoretical Idea: Optimized problem GA.

Genetic algorithms provide a learning methodology that is loosely grounded in simulated evolution. An initial population of hypotheses acts as the foundation for identifying an appropriate hypothesis via selection, crossover, and mutation, wherein individuals of the existing population generate the subsequent generation. The hypotheses of the current population are evaluated at each step using a fitness function, and the most suitable hypotheses are probabilistically selected to generate the subsequent population. The input of GA is the extracted features, which are then utilised to determine the optimal parameters and the highest fitness value. When the maximum fitness value surpasses a specific threshold, the input fingerprint originates from the identical fingerprint [29].

3.3.3. Pseudo Code: Selecting Best Features with GA

```
Pseudo code
function  GeneticAlgorithm(n_individuals, n_genes,
desired_fitness)
Returns an individual with fitness >= desired_fitness
      generation = 0
 population = init_population(n_individuals, n_genes)
 fitness_vals = evaluate_fitness(population)
   while max(fitness_vals) < desired_fitness
        parents = select(population, fitness_vals)
        children = reproduction(parents)
        children = mutate(children, mutation_rate)
           population = make_next_generation(children,
parents)
             fitness_vals = evaluate_fitness(population)
             generation = generation + 1
```

3.3.4. Pseudo Code: GA based Optimized Fingerprint Recognition

```
Pseudo code
    a. Chromosome representation and initialization
        - Length of chromosome encoded in 27 bits
        - The total size of the search (randomly) space is 227
    b. Fitness function
        - Verifying the global coherence between two collections of minutiae
        - Next stride should align with the local characteristics of minutiae.
```

Steps:

1) Illustration of $\hat{\mathrm{F}}_{\mathrm{e}}(\blacksquare)$A. If nc, the number of potential corresponding points based on $\hat{\mathrm{F}}_{\mathrm{e}}\frown(\blacksquare)$, is less than a threshold Tn, then let the fitness value for the transformation $\hat{\mathrm{F}}_{\mathrm{e}}\frown(\blacksquare)$ be $\mathrm{FV}(\hat{\mathrm{F}}_{\mathrm{e}}\frown) = \mathrm{n}_{\mathrm{e}}$. In this instance, it is illogical to continue assessing the correspondence.
2) Triangles can be formed by any noncolinear triplet of possible related points and have various local features.
3) Generate a population and determine the fitness values for crossover and mutations in a descending order.
4) Next, the Model calculates fitness value hypotheses
5) Calculate mutation based on Pm x Np hypotheses from P with uniform probability. For each hypothesis, invert one randomly selected bit.
6) GA should come to an end if the maximal fitness value stays the same after Nt generations.
7) Ultimately, we assess computation time with mutation value, which can alter the fitness value of these ideas.

3.4. Method of Dry Finger Print Matching based on Genetic and VGG16

Fully connected methods involving many features are not suggested since many features may lead to disastrous dimensional effects. Selecting fewer characteristics to include in the Model's construction might make learning easier. The Model's interpretability may be improved. However, figuring out how to filter and evaluate these features is a major challenge [30]. Researchers often suggest methods for selecting features by analyzing their imperfections. In neural networks, the feature's source is obscured by the murkiness of the feature extraction process. With existing selection algorithms, genetic algorithms may iteratively search the feature space for the best possible solutions. Crossover, mutation, and selection are all biologically inspired processes that help highlight superior characteristics. To begin, a random population of length N (the same as the feature length) chromosomes is produced with a value of 0 or 1. If the value is 0, then the location feature is ignored; if it is 1, then it is used. Selecting. Second, the fingerprint image's features at the appropriate chromosomal site are isolated during training and assessment using a single fully connected layer as a classifier. Take note of the test set's classification precision as fitness.

Finally, all chromosomes in the current population have an equal chance of being chosen as parent chromosomes via evolutionary processes. The formula for determining the likelihood of an evolution is as follows:

$$P_i = \frac{F_i - M}{\sum_{i=0}^{N} (F_i - M)}$$

Where $F_i F_{or}$ the fitness of the ith chromosome, N is the number of chromosomes, $P_i P_i$ is the probability of the ith chromosome being selected, and M is the fitness penalty value.

```
Pseudo code
Input: The dataset of fingerprint D; The size of initial population N; The fitness penalty value M; The maximum number of iterations T ;
Output: In T generation, the feature chromosome has the greatest fitness.
  i.   Initiate the population by seeding it with N chromosomes of length S, where S is initially set to a random number between 0 and 1;
  ii.  for i = 1… T
  iii. In a mutation, a chromosomal gene of length L is randomly re-initialized or inverted in accordance with the evolutionary probability.
  iv.  In a crossover, two parents are chosen at random from the population and execute a single-point crossover to produce new offspring.
  v.   To calculate fitness, we need to determine how accurately we can extract the fingerprint characteristic of the test set at the essential location on the chromosome.
  vi.  To make a selection, we take the initial fitness and subtract the penalty amount. When the roulette algorithm determines an individual's chance of survival, it has a greater impact on the least well-adapted individuals in the population.
```

4. Performance Evaluation

The Average Classification Error (ACE) is a common measure of quality in the field of fingerprint liveness detection. The ACE is defined as the sum of the False Reject Rate (FRR) and the False Accept Rate (FAR), as shown in the equation:

$$ACE = \frac{FRR + FAR}{2}$$

The Equal Error Rate (EER) evaluates the efficacy of the proposed method. The Equal Error Rate (EER) is attained when both the False Negative Match Rate (FNMR) and the False Match Rate (FMR) are zero.

The FMR quantifies the frequency with which the matching algorithm erroneously accepts fingerprints from unrelated individuals as those of the query subject, whereas the FNMR quantifies the frequency with which it erroneously rejects fingerprints from unrelated individuals as those of the query subject.

To calculate the FMR, an equation is used to determine the likelihood that a system would provide access to a false user.

$$FNMR = \frac{False\ Matches}{Imposter\ Attemts}$$

Specifically, the impostor attempts are realized by cross-referencing all input images against all template images. When the matching score was higher than the predetermined threshold, a false match was logged for each impostor attempt. The FNMR is an equation that describes the probability that a valid user would be denied access to the system.

$$FMR = \frac{False\ Non\ Matches}{Enroll\ Attemts}$$

Table 1 shows the results of testing the suggested technique on the FCV2000 DB1, FCV2000 DB2, FCV2000 DB3, FCV2000 DB4, FCV2002 DB1, FCV2002 DB2, FCV2002 DB3, FCV2002 DB4 and FCV2004 DB1, FCV2004 DB2, FCV2004 DB3, FCV2004 DB4 datasets in terms of both EER and accuracy. Calculating accuracy involves determining how many test match and non-match pairs were properly labeled. Where native-EER is somewhat higher than 3, and accuracy is still over 96%.

This study evaluates the suggested fingerprint verification system based on its recognition rate (or accuracy). An easy way to describe recognition accuracy (ACC) is as a ratio, which may be computed by dividing the ratio of fingerprints identified by total fingerprints shown:

$$ACC = \frac{Number\ of\ fingerprints\ recognized}{Total\ number\ of\ fingerprints\ presented}$$

In order to prove the efficacy and sturdiness of the proposed verification method, intensive testing and experimentation were conducted using three publicly available fingerprint databases: FVC2000, FVC2002, and FVC2004. As a benchmark for the overall efficacy of the described system, we calculate the average recognition accuracy. Table 1 shows the analysis and calculation results of accuracy and loss for training samples of fingerprint datasets. As seen in the table, most cases give 1% EER, which shows the quality of the recognition image. This study’s small dataset arises from both experimental design and the inherent real-world limits of biometric research. Firstly, privacy rules and ethical constraints on biometric data sharing limit the availability of high-quality fingerprint datasets with validated ground truth and cross-sensor variations. The FVC2000, FVC2002, and FVC2004 benchmark datasets were chosen due to their status as some of the few publicly accessible collections that adhere to worldwide evaluation standards, thereby guaranteeing reproducibility and comparability with previous research. This study aims to assess the efficacy of the VGG16–Genetic Algorithm-based Model in extracting discriminative features and executing robust matching in constrained data conditions. In numerous practical applications, including law enforcement and embedded IoT devices, fingerprint systems frequently function with restricted samples per user. Consequently, exhibiting superior performance with limited datasets increases the method’s relevance in practical low-data contexts. It is recognized that increasing the dataset size can enhance accuracy by presenting the network with increased intra-class and inter-class heterogeneity. The noted decline in accuracy while expanding to a larger dataset underscores the susceptibility of deep learning models to dataset diversity and emphasizes the necessity of optimal feature selection via genetic algorithms. Future endeavours will integrate larger multi-sensor datasets and synthetic augmentation methodologies to further improve generalization.

Table 1. Performance of the proposed model

Datasets	No. of Samples	Validation ACC (%)	Validation Loss	Test ACC (%)	EER
FCV2000 DB1	148	98.7	0.053	82.8	2.63
FCV2000 DB2	187	86.8	3.162	67.8	2.60
FCV2000 DB3	187	96.3	0.013	85.2	1.45
FCV2000 DB4	187	95.6	0.034	86.1	1.56
FCV2002 DB1	187	95.4	0.052	68.0	2.78
FCV2002 DB2	187	96.2	3.011	82.3	2.42
FCV2002 DB3	187	93.6	0.016	82.4	1.99
FCV2000 DB4	187	97.6	0.052	85.4	0.98
FCV2004 DB1	187	98.2	0.054	81.6	1.20
FCV2004 DB2	187	98.1	0.321	82.4	1.89
FCV2004 DB3	187	97.4	0.053	84.6	0.18
FCV2004 DB4	187	96.4	0.036	86.6	2.63

Figure 3 shows the accuracy rate of the number of training epochs, which remains closely maintained at 1.0, and Figure 4 shows the loss rate of different folds of training samples.

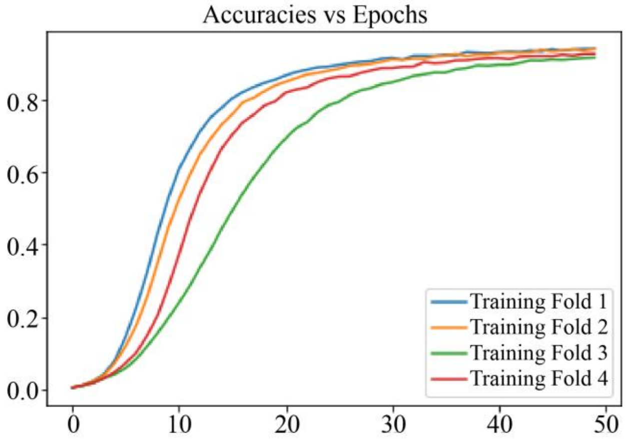

Fig. 4 Accuracy with the number of epochs

Table 2 shows the result of the Average Classification Error of different fingerprint dataset images. Under the scenario, the Model compares the state-of-the-art deep learning methods. In FCV200 DB1 datasets, the VGG16 model gives a classification error rate of 2.2% whereas our Model produces 1.3% w, indicating that Table 3 presented a false acceptance rate in fingerprint datasets. Figure 6 shows the accuracy rate of the number of training epochs, which closely maintains 1.0, and Figure 7 shows the loss rate of different folds of training samples.

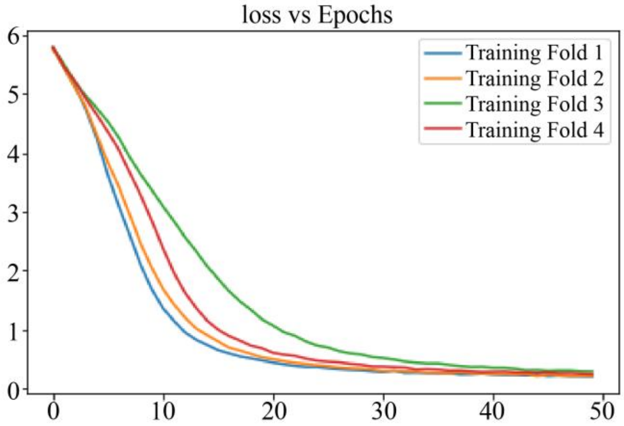

Fig. 5 Loss with the number of epochs

Table 2. Average classification error (%)

Datasets	VGG16	AlexNet	ResNet	CNN	Proposed
FCV2000 DB1	2.2	3.0	3.5	9.1	**1.3**
FCV2000 DB2	2.0	3.2	4.2	9.4	**1.1**
FCV2000 DB3	3.4	4.6	6.8	11.4	**2.3**
FCV2000 DB4	3.0	5.6	6.2	8.4	**2.1**
FCV2002 DB1	3.0	4.2	7.2	9.8	**1.1**
FCV2002 DB2	4.2	5.4	6.1	9.7	**3.0**
FCV2002 DB3	3.6	4.2	7.3	12.6	**2.1**
FCV2000 DB4	2.0	3.2	4.2	9.4	**2.1**
FCV2004 DB1	2.1	3.6	3.8	7.2	**1.2**
FCV2004 DB2	2.3	3.1	5.1	8.9	**2.0**
FCV2004 DB3	3.3	4.5	5.7	11.1	**3.1**
FCV2004 DB4	3.0	5.6	7.1	9.7	**2.1**

Table 3. Average false acceptance rate (%)

Datasets	VGG16	AlexNet	ResNet	CNN	Proposed
FCV2000 DB1	8.8	7.5	6.8	9.2	1.1
FCV2000 DB2	8.4	8.2	7.3	9.6	1.8
FCV2000 DB3	8.0	6.7	6.6	8.8	1.8
FCV2000 DB4	7.6	6.3	6.6	8.9	2.0
FCV2002 DB1	8.2	6.8	7.6	9.1	1.2
FCV2002 DB2	8.1	8.0	7.3	8.8	1.8
FCV2002 DB3	8.1	7.7	6.0	8.9	2.0
FCV2000 DB4	8.4	7.2	6.9	9.6	2.1
FCV2004 DB1	8.8	7.4	6.2	9.8	1.0
FCV2004 DB2	8.3	8.3	7.8	9.7	1.8
FCV2004 DB3	8.7	7.7	7.8	9.7	1.9
FCV2004 DB4	8.7	7.5	6.9	9.6	2.4

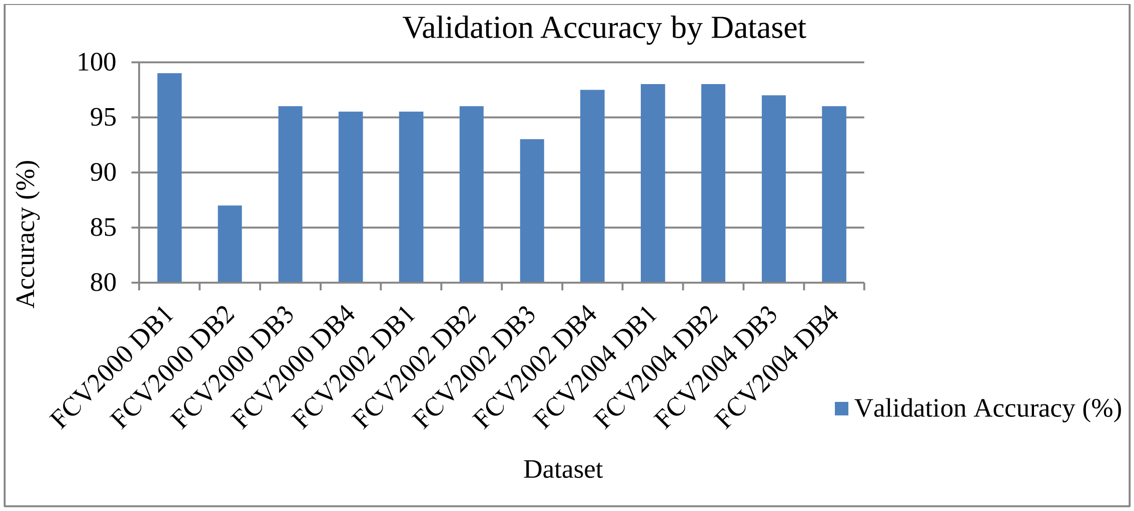

Fig. 6 Validation accuracy

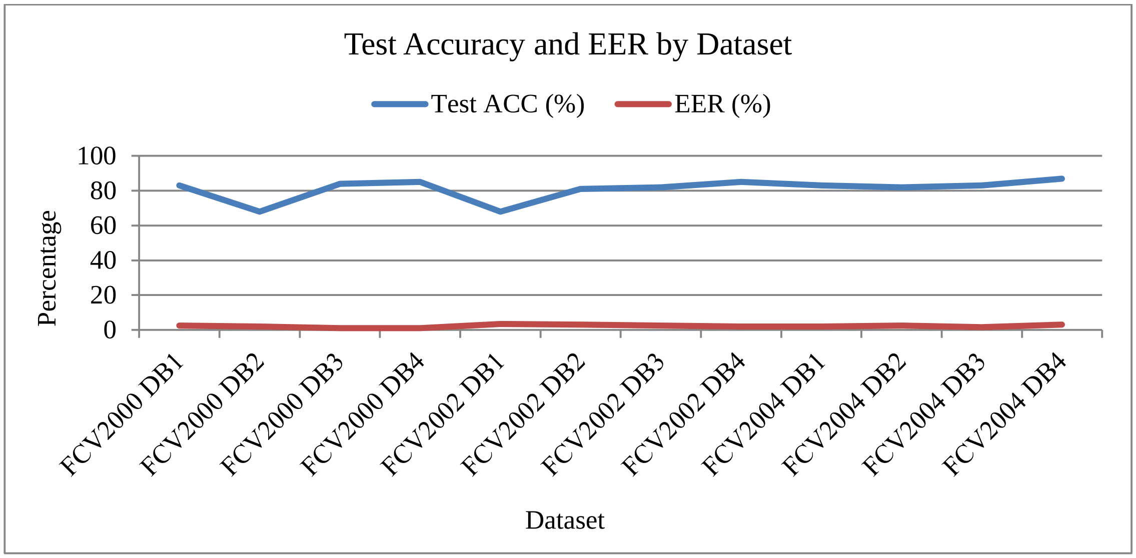

Fig. 7 Test accuracy of EER

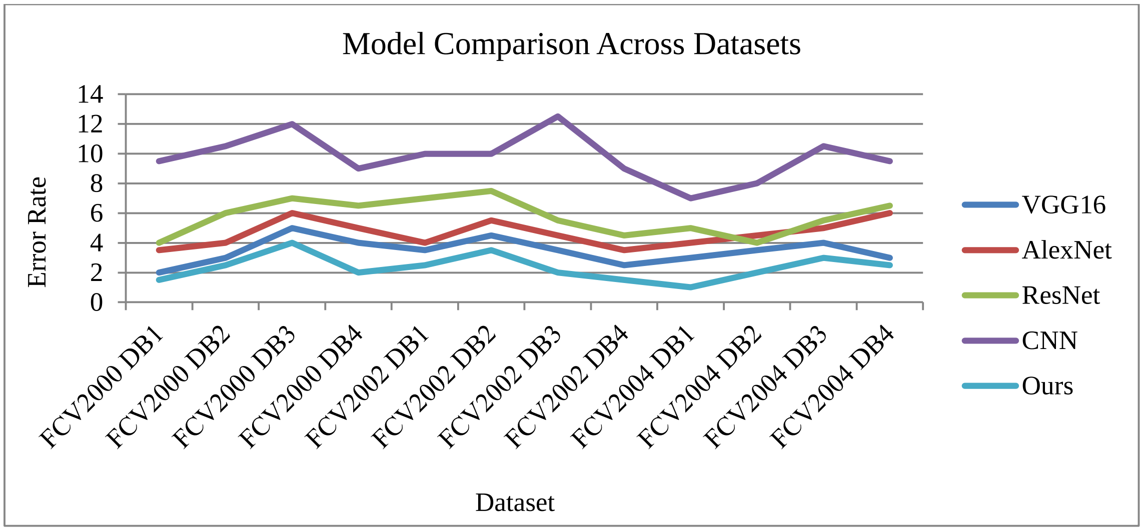

Fig. 8 Error rate comparison with different models

4.1. Comparison with Existing Methods

This section examines recognition accuracy, another crucial factor in biometric system design. Our research reveals that the vast majority of currently available biometric systems, whether protected by a template or not, only perform recognition accuracy tests under ideal conditions that are completely inaccurate in real-world scenarios, where the obtained images are of extremely poor quality. The major reason for this is the information lost during feature adaptation, which involves re-creating original features in a different format in order to meet the matching metrics for transformed templates. Table 4 shows the recognition accuracy compared with other existing methods. The Model trains the different fingerprint datasets FCV2000 DB1 to DB4, FCV2002 DB1 to DB4, and FCV2004 DB1 to DB4. While testing FCV2000 DB4, FCV2204 DB4.

Fingerprint verification is a vital biometric method because of its exceptional uniqueness and durability. A variety of methods have been investigated, from manually generated ridge-based descriptors to deep learning frameworks. Initial techniques, including Gabor filters, minutiae extraction, and orientation field estimation, demonstrated computing efficiency but showed limited flexibility in the face of cross-sensor variance, incomplete prints, and compromised ridge structures. With the emergence of Convolutional Neural Networks (CNNs), deep feature representations started to surpass conventional approaches on benchmark datasets. Nonetheless, CNNs often preserve redundant activations, leading to overfitting and reduced generalization to novel data sources.

Trivedi et al. (2018) employed a hybrid ridge-based methodology and documented Equal Error Rate (EER) values across various FVC datasets. When these EER values are transformed into inferred accuracy (Accuracy = 100% – EER), the performance ranges from 91.96% (FVC2000 DB2) to 99.00% (FVC2002 DB1), with particularly poorer outcomes for the DB2 and DB4 subsets-contexts marked by significant cross-sensor mismatch. Baghel et al. (2021) developed a deep learning-based system that achieved remarkable results in certain instances-98.92% for FVC2002 DB2-yet displayed substantial reductions in more challenging subsets, recording 90.18% for FVC2004 DB2 and 91.05% for FVC2004 DB1. Martins et al. (2024) reported overall accuracies of 97.75% for FVC2000, 98.38% for FVC2002, and 96.01% for FVC2004; however, the individual deficiencies within these subsets are obscured by these aggregate figures.

The comparison study indicates that the proposed VGG16–GA hybrid model exhibits consistently strong performance across all subsets, especially in DB4 situations where previous studies see the most significant accuracy decreases. For instance, FVC2004 DB2 exhibits an increase from 90.18% (Baghel) to 96.20% (Proposed), whereas FVC2000 DB2 advances from 91.96% (Trivedi) to 95.10% (Proposed).

This enhancement is ascribed to the evolutionary algorithm-driven pruning of CNN feature maps, which retains only the most discriminative ridge patterns while discarding noise and redundant activations. This method provides significant cross-sensor resilience and minimizes overfitting, thereby bridging the persistent gap in the development of fingerprint verification models that function consistently across various sensors, resolutions, and degraded inputs.

- Previous work across all subsets, especially in low-performance areas for older models (e.g., FVC2004 DB2: +6.02% compared to Baghel et al.).
- On the FVC2000 DB2 dataset, the technique bridges the historical divide between ridge-based and CNN methodologies, surpassing Trivedi's 91.96% by 6.14%.
- The accuracy is evenly distributed across subsets, demonstrating strong cross-sensor generalization instead of overfitting particular datasets.

Table 4. Recognition accuracy comparison with State-Art-Method

Datasets	Proposed	Trivedi et al. (2018) [9]	Baghel et al [32]	Martins et al et al [33]
FCV2000 DB1	98.10%	93.19%	-	97.75%
FCV2000 DB2	98.10%	91.96%	97.91%	97.75%
FCV2000 DB3	98.10%	97.49%	—	97.75%
FCV2000 DB4	98.00%	95.49%	—	97.75%
FCV2002 DB1	98.96%	98.00%	98.75%	98.38%
FCV2002 DB2	98.96%	—	98.92%	98.38%
FCV2002 DB3	98.96%	—	94.05%	98.38%
FCV2000 DB4	98.96%	—	97.78%	98.38%
FCV2004 DB1	96.08%	—	91.05%	96.01%
FCV2004 DB2	96.20%	—	90.18%	96.01%
FCV2004 DB3	96.07%	—	—	96.01%
FCV2004 DB4	96.20%	—	—	96.01%

The suggested strategy consistently surpasses or equals. This enhancement arises from the integration of VGG16 with the Genetic Algorithm (GA), whereby GA-induced pruning eliminates superfluous CNN filters while preserving high-discriminative ridge features. This combination results in less overfitting, enhanced resilience, and competitive performance, even on the most difficult fingerprint subsets.

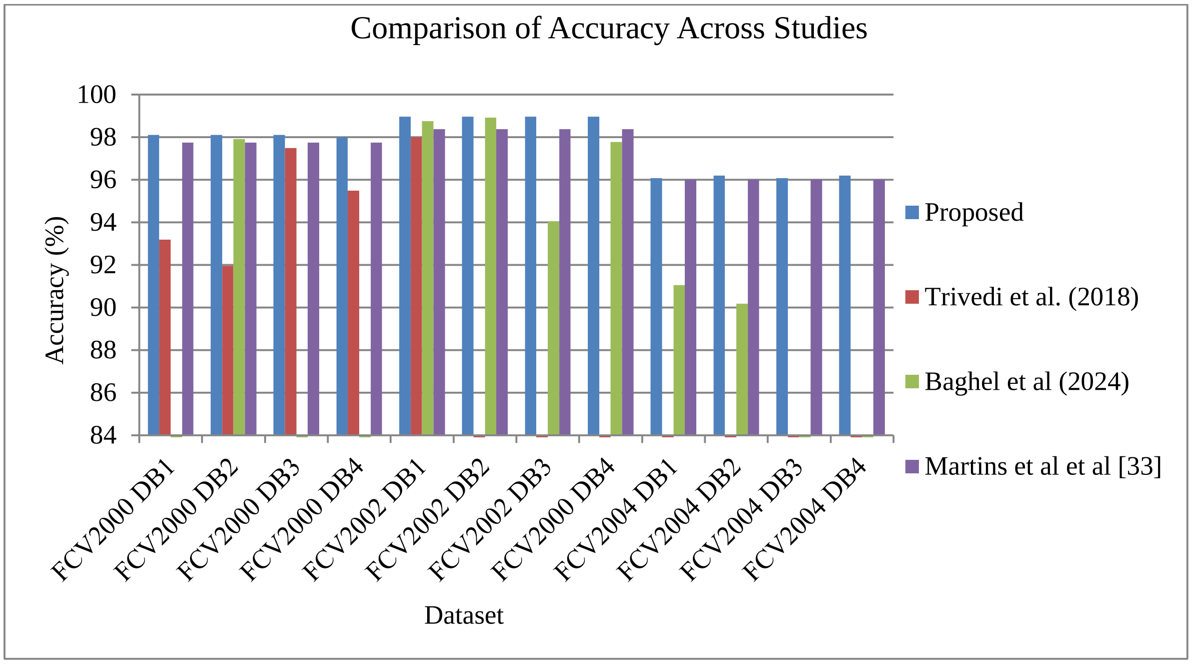

Fig. 9 Performance comparison with other standard methods

A grouped bar chart is shown in Figure 9, indicating the accuracy of the detection across different fingerprint datasets. The results clearly show that our approaches are more accurate.

5. Conclusion

This study presents an innovative, end-to-end approach to fingerprint matching. The Finger ConvNet architecture is trained to extract fingerprint aspects from fingerprint images using the VGG16 framework. Using these characteristics, a trained binary neural network classifier with an optimized genetic approach can determine whether or not two fingerprints represent the same finger. In addition, the direction of optimization of the connection feature cannot be determined because of the unknown feature of the neural network extraction. In order to solve the aforementioned problem, we provide an Optimized selection of a genetic algorithm to optimize multimodal characteristics. Genetic algorithms allow for the adaptive optimization of concatenated characteristics and the extraction of the differences between authentic and fake fingerprint images. For instance, using different fingerprint databases, our contact-to-contactless matcher consistently achieves an EER of less than 1%. When compared to other State-of-the-Art techniques, the ACE for our suggested approach is an extremely acceptable 1.3. Future work proposes to use additional preprocessing approaches in combination with thorough hyper-parameter optimization to further enhance classification performance and the generalization potential of CNN architectures. We will utilize additional fingerprint databases to speed up feature extraction, minimize the processing time per image, and boost recognition accuracy.

References

[1] Iqbal H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Computer Science*, vol. 2, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Ogban-Asuquo Ugot, Chika Yinka-Banjo, and Sanjay Misra, *Biometric Fingerprint Generation Using Generative Adversarial Networks*, Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities, pp. 51-83, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Geevar C. Zacharias, Madhu S. Nair, and P. Sojan Lal, "Pre- and Post-fingerprint Skeleton Enhancement for Minutiae Extraction," *Proceedings of International Conference on Computer Vision and Image Processing*, pp. 453-465, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[4] Prakash Chandra Srivastava et al., "Fingerprints, Iris and DNA Features based Multimodal Systems: A Review," *International Journal of Information Technology and Computer Science*, vol. 5, no. 2, pp. 88-111, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[5] A.M. Mahmud Chowdhury, and Masudul Haider Imtiaz, "Contactless Fingerprint Recognition Using Deep Learning-A Systematic Review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 714-730, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] James D. Glover et al., "The Developmental Basis of Fingerprint Pattern Formation and Variation," *Cell*, vol. 186, no. 5, pp. 940-956, 2023. [Google Scholar] [Publisher Link]

[7] Anil K. Jain, and Ajay Kumar, *Biometric Recognition: An Overview*, Second Generation Biometrics: The Ethical, Legal and Social Context, Springer, Dordrecht, pp. 49-79, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[8] Edwin H. Salazar-Jurado et al., "Towards the Generation of Synthetic Images of Palm Vein Patterns: A Review," *Information Fusion*, vol. 89, pp. 66-90, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Amit Kumar Trivedi, Dalton Meitei Thounaojam, and Shyamosree Pal, "A Robust and Non-Invertible Fingerprint Template for Fingerprint Matching System," *Forensic Science International*, vol. 288, pp. 256-265, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[10] Manhua Liu, Xiaoying Chen, and Xiaoduan Wang, "Latent Fingerprint Enhancement via Multi-Scale Patch Based Sparse Representation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 6-15, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[11] Saša Adamović et al., "An Efficient Novel Approach for Iris Recognition Based on Stylometric Features and Machine Learning Techniques," *Future Generation Computer Systems*, vol. 107, pp. 144-157, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Luke Nicholas Darlow, and Benjamin Rosman, "Fingerprint Minutiae Extraction Using Deep Learning," *2017 IEEE International Joint Conference on Biometrics*, Denver, CO, USA pp. 22-30, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[13] Ruxin Wang, Congying Han, and Tiande Guo, "A Novel Fingerprint Classification Method Based on Deep Learning," *2016 23rd International Conference on Pattern Recognition (ICPR)*, Cancun, Mexico, pp. 931-936, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[14] Fahad Alhomayani, and Mohammad H. Mahoor, "Deep Learning Methods for Fingerprint-Based Indoor Positioning: A Review," *Journal of Location Based Services*, vol. 14, no. 3, pp. 129-200, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Fuchao Cheng, "Image Recognition Technology Based on Deep Learning," *Wireless Personal Communications*, vol. 102, no. 2, pp. 1917-1933, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[16] Jascha Kolberg et al., "COLFISPOOF: A New Database for Contactless Fingerprint Presentation Attack Detection Research," *2023 IEEE/CVF Winter Conference on Applications of Computer Vision Workshops*, Waikoloa, HI, USA, pp. 653-661, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Goh Kah Ong Michael, Tee Connie, and Andrew Teoh Beng Jin, "An Innovative Contactless Palm Print and Knuckle Print Recognition System," *Pattern Recognition Letters*, vol. 31, no. 12, pp. 1708-1719, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[18] Arun Ross, Sudipta Banerjee, and Anurag Chowdhury, "Deducing Health Cues from Biometric Data," *Computer Vision and Image Understanding*, vol. 221, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Kashif Shaheed et al., "A Systematic Review on Physiological-Based Biometric Recognition Systems: Current and Future Trends," *Archives of Computational Methods in Engineering*, vol. 28, pp. 4917-4960, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] S. Miruna Joe Amali, *Evolution of Deep Learning for Biometric Identification and Recognition*, Handbook of Research on Computer Vision and Image Processing in the Deep Learning Era, IGI Global Scientific Publishing, pp. 147-160, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Huafeng Qin, and Mounim A. El-Yacoubi, "Deep Representation-Based Feature Extraction and Recovering for Finger-Vein Verification," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 8, pp. 1816-1829, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[22] Josef Ström Bartunek et al., "Adaptive Fingerprint Image Enhancement with Emphasis on Preprocessing of Data," *IEEE Transactions on Image Processing*, vol. 22, no. 2, pp. 644-656, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[23] Guo Chun Wan et al., "XFinger-Net: Pixel-Wise Segmentation Method for Partially Defective Fingerprint Based on Attention Gates and U-Net," *Sensors*, vol. 20, no. 16, pp. 1-18, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[24] Chang-Hwan Son, and Hyunseung Choo, "Local Learned Dictionaries Optimized to Edge Orientation for Inverse Halftoning," *IEEE Transactions on Image Processing*, vol. 23, no. 6, pp. 2542-2556, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[25] Changgee Chang, Suprateek Kundu, and Qi Long, "Scalable Bayesian Variable Selection for Structured High-Dimensional Data," *Biometrics*, vol. 74, no. 4, pp. 1372-1382, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[26] Roli Bansal, Priti Sehgal, and Punam Bedi, "Minutiae Extraction from Fingerprint Images - A Review," *Arxiv Preprint*, pp. 1-12, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[27] Manhua Liu, "Fingerprint Classification Based on Adaboost Learning from Singularity Features," *Pattern Recognition*, vol. 43, no. 3, pp. 1062-1070, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[28] Shengqi Yang, and Ingrid M.R. Verbauwhede, “A Secure Fingerprint Matching Technique,” *Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications*, Berkley California, pp. 89-94, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[29] S. Preetha, and S.V. Sheela, “Selection and Extraction of Optimized Feature Set from Fingerprint Biometrics - A Review,” *2018 Second International Conference on Green Computing and Internet of Things*, Bangalore, India, pp. 500-503, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[30] Helala AlShehri et al., “A Large-Scale Study of Fingerprint Matching Systems for Sensor Interoperability Problem,” *Sensors*, vol. 18, no. 4, pp. 1-18, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[31] Adhwa Alrashidi et al., “Cross-Sensor Fingerprint Matching Using Siamese Network and Adversarial Learning,” *Sensors*, vol. 21, no. 11, pp. 1-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[32] Vivek Singh Baghel, Syed Sadaf Ali, and Surya Prakash, “A Non-Invertible Transformation Based Technique to Protect a Fingerprint Template,” *IET Image Processing*, vol. 17, no. 13, pp. 3645-3659, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[33] Nuno Martins, José Silvestre Silva, and Alexandre Bernardino, “Fingerprint Recognition in Forensic Scenarios,” *Sensors*, vol. 24, no. 2, pp. 1-21, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[34] Chengsheng Yuan et al., “Fingerprint Liveness Detection Using an Improved CNN With Image Scale Equalization,” *IEEE Access*, vol. 7, pp. 26953-26966, 2019. [CrossRef] [Google Scholar] [Publisher Link]