Journal of Al-Qadisiyah for Computer Science and Mathematics Vol. 15(3) 2023 , pp Comp. 126–142

Available online at www.qu.edu.iq/journalcm

JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS

ISSN:2521-3504(online) ISSN:2074-0204(print)

Optimization Techniques for Human Multi-Biometric Recognition System

Maryam Yaseen Abdullah

Department of Computer Science, College of Education for Women, University of Baghdad, Iraq,maryam84@coeduw.uobaghdad.edu.iq

A R T I C L E I N F O

Article history:
Received: 10 /07/2023
Rrevised form: 25 /08/2023
Accepted : 29 /08/2023
Available online: 30 /09/2023

Keywords:
Biometric system
Feature selection
Metaheuristic optimization algorithms
Machine learning

A B S T R A C T

Researchers are increasingly using multimodal biometrics to strengthen the security of biometric applications. In this study, a strong multimodal human identification model was developed to address the growing problem of spoofing attacks in biometric security systems. Through the use of metaheuristic optimization methods, such as the Genetic Algorithm(GA), Ant Colony Optimization(ACO), and Particle Swarm Optimization (PSO) for feature selection, this unique model incorporates three biometric modalities: face, iris, and fingerprint. Image pre-processing, feature extraction, critical image feature selection, and multibiometric recognition are the four main steps in the workflow of the system. To determine its performance, the model was evaluated on the SDUMLA-HMT dataset, which contains a variety of biometric features from various individuals. The system outperformed existing techniques in the literature with an excellent recognition accuracy of 99.4%. Although this result is encouraging, further research on larger and more varied datasets is necessary to confirm its applicability across many circumstances. This study highlights how multimodal biometrics strengthened by metaheuristic algorithms can considerably increase biometric security against spoofing assaults, thereby opening a promising new direction for future development in the field.

https://doi.org/10.29304/jqcsm.2023.15.31292

1. Introduction

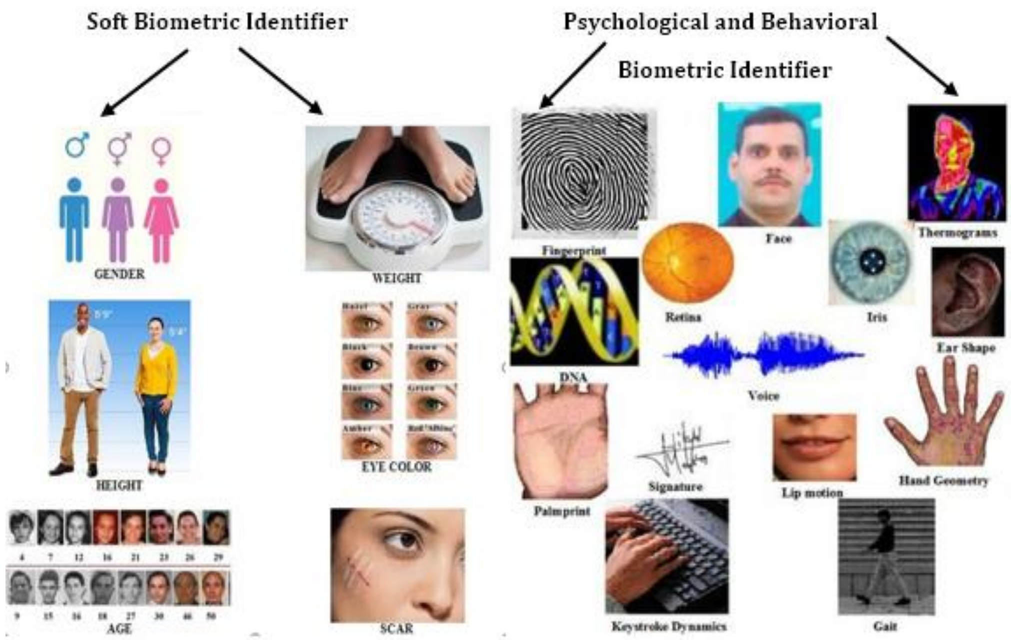
Nowadays, our society is electronically connected and depends on mobile devices for many applications that require a stronger security system. Thus, the traditional methods for person identification, such as passwords and tokens, cannot be trusted. Recent studies have used human biometric methods to provide high-level convenient security systems [1][2]. It identifies a person based on their physiological or behavioral traits (walk, fingerprint, face, iris, voice, lip print, etc.).

The recognition of a person by estimating his traits of individual anatomy and physiological features has caused a marked research area called biometric recognition. Biometric technologies provide a powerful mechanism for person authentication, and this research area is still under continual development. Their use is fundamentally propped by government and law enforcement to improve public security.

∗Maryam yaseen abdullah
Email addresses: *maryam84@coeduw.uobaghdad.edu.iq*

Communicated by ‘sub etitor’

Diverse types of biometric traits can be utilized in person authentication or recognition systems. All biometric traits are grouped into physiological, behavioral, and soft biometrics [3][4]. Under these three categories, a variety of biometric traits is specified. From these biometric categories, any number of biometric traits can be used in multimodal biometric recognition systems. Fig. 1 shows three groups of biometric traits [5][6].



(a) (b)

Fig. 1 - Biometric traits(a) [5], (b) [6]

Unimodal systems, which are a unique source of data in biometric systems, are flawless, but frequently have issues when dealing with noisy data, such as intra-class variances, constrained degrees of freedom, and non-universality. Utilizing multimodal biometric systems also known as "Biometric Fusion" systems which combine two or more biometrics can help alleviate a number of these issues. There can be (N) a number of different biometrics that can be fused. Owing to the high degree of sophistication in the formation architecture, a fused biometric classification is superior to a unimodal biometric classification. Information fusion in multimodal systems can be accomplished using various techniques, fusion levels, and integration methodologies [7].

The information accessible in one of the biometric system modules can be used to combine many qualities in multimodal biometric systems. There are five biometric fusion methods (rank-, feature-, decision-, sensor-, and score-level fusion). To recognize several biometrics, researchers have used machine-learning techniques [8]. Before classifying the raw biometric data, machine learning algorithms must transform them into a suitable format and extract characteristics or features from it. Thus, extracting the best features to represent human biometrics is a vital step in designing an accurate biometric recognition system [9].

In the current research, metaheuristic algorithms, such as Particle Swarm Optimization, Genetic Algorithm and Ant Colony Optimization, are utilized to select the best biometric features.

1.1. Motivation

Fake and counterfeit technologies have been developed and spread widely in society. Consequently, identifying a human biometric that is difficult to fabricate is essential. Thus, the fusion of many biometrics can provide an accurate and difficult-to-penetrate recognition system.

1.2. Contribution

The main contribution of this study is the proposal of an automatically accurate multi-biometric recognition method. A novel feature of multibiometrics (face, iris, and fingerprint) was introduced based on metaheuristic optimization. The optimization methods (GA, ACO, and PSO) significantly affect the selection of dominant features that are fed to the classification algorithm.

1.3. Paper organization

The remainder of this paper is organized as follows. Related work is discussed in Section 2. In Section 3, the proposed multibiometric recognition method is described in detail. The experimental results of the proposed method are presented in Section 4. In Section 5, we conclude the paper from several perspectives.

2. Related Work

Donghoon Chang et al [10],2021, emphasized the possibility of biometric authentication technologies to increase security over current practices. They discussed the procedure for collecting distinctive physical or behavioral characteristics as biometric data. However, they acknowledged the difficulties in maintaining long-term security of such data.

Garg et al. [11],2020, focused on the problem of multimodal biometric fusion to increase recognition security. This study uses speech, iris, and signature to create a revolutionary fusion. For each biometric, a separate classification mechanism was also presented. Fusion is performed using features taken out of each biometric during individual classification. Multiple feature-extraction techniques have been used for various biometrics. Their study uses mel-frequency spectral coefficients for speech biometrics, Scale Invariant Feature Transform (SIFT) for signatures, and two-dimensional principal component analysis (2DPCA) for iris analysis. A (GA) is used in this study to optimize the evaluated features. Artificial Neural Networks are used for classification (ANN).

S. Sengar, Hariharan, and Rajkumar [12],2021, Their proposed system is based on multimodal biometrics, in which palmprint and fingerprint data are employed as a source of authentication. An " automated fingerprint identification system " (AFIS) employs techniques that are often based on the concentration of specific information. Using multimodal biometrics, it is consistently possible to achieve the goal of creating a secure unique identification device. The highest level of accuracy is achieved by palm and fingerprints that are rich in floor information. DNN grounded distinction results in a good identification fee.

Vinothkanna and Wahi[13] ,2020, They proposed employing a fuzzy vault to recognize palm print, hand vein, and finger print using a multimodal biometric technique. These pictures were initially preprocessed to remove undesirable elements and reduce noise levels. The pre-processed image was then used to extract the features. The chaff points and extracted feature points are then combined to create a single feature vector point. The fuzzy vault is created by combining the combined feature vector point with the points generated by the secret key. The authentication of a person is granted, and a secret key is created if their total feature vector matches that of the fuzzy vault. The fingerprint, hand vein, and palmprint databases were used in the experiment, and the results showed that the proposed technique produced improved recognition with 98.5% accuracy.

Kumar et al. [14],2021, proposed the fusing of features of face and fingerprint recognition systems as an" Improved Biometric Fusion System' (IBFS), resulting in increased performance. Integrating multibiometric attributes enhances recognition performance, which lowers unauthorized access. This work introduces an IBFS that includes an ' improved face recognition system' (IFRS) and ' improved fingerprint recognition system' (IFPRS) for authentication. For IFPRS and IFRS, the whale optimization algorithm is combined with the details feature and 'Maximally Stable External Regions' (MSER). The planned IBFS was trained using a classification approach called the pattern-net model. The IBFS model is trained using pattern networks that depend on a processed dataset and an SVM to improve classification accuracy. The average true-positive rate and accuracy of the suggested fusion system were 99.8 and 99.6 percent, respectively.

Mohammed et al. [15], delved deeply into the individual identification potential of multi-biometric fusion. The Dis-Eigen algorithm is a novel feature-level algorithm. Here, a feature fusion architecture is suggested to improve the accuracy when using various biometrics to identify a person. The framework, which directs multibiometric fusion implementations at the feature level for identifying individuals, thus serves as the foundation for the new multibiometric system. This framework used the face and fingerprints of 20 people, each represented by 160 photos. The experimental results of the suggested methodology revealed a feature-level fusion multibiometric individual detection rate of 93.70 percent.

Despite this, many studies have investigated fusion biometric or multibiometric recognition. However, there are gaps in addressing this issue.

• Design an automatic multibiometric identification system that is easy to implement, and at the same time, its performance is accurate.

• Determining the best features that can be used to represent human biometrics.

• Application of metaheuristic optimization algorithms for biometric feature selection

3-The Proposed System

In this section, we describe in detail the proposed system for person identification or recognition using multibiometric images. An automated system has the advantage of fetching technology for wider global use and opening up a door for the potential development of functional security software. Fig.2. displays a block diagram of the proposed system. Each block is described in detail in the following subsection.

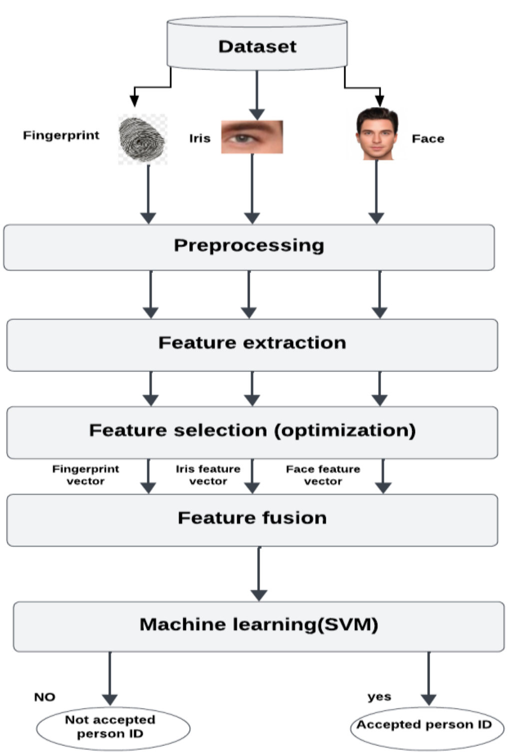


Fig .2- The proposed system diagram.

3.1. Dataset

The SDUMLA-HMT dataset contains different human biometrics and was prepared by Shandong University. SDUMLA-HMT contain a biometric data of 106 people. The data included the iris, face, fingerprint, finger vein biometric image, and gait biometrics. SDUMLA-HMT has 1060 images of iris were captured by a smart iris capture device, this device designed by the University of Science and Technology of China. In addition, SDUMLA-HMT includes 8904 face images on different sides of the pose, facial expressions, and illumination. In addition, SDUMLA-HMT has 25,440 fingerprint images that were collected by an efficient device developed by the Intelligent Computing and System Labs of Wuhan University [16].

3.2 Preprocessing

In this stage, each biometric image (fingerprint, iris, and face) is improved in quality and noise is reduced using a variety of techniques [17]. Each pixel value was rounded with respect to its neighbors using a median filter. The photos were then downsized to 224 × 244 pixels using interpolation techniques.

3.3 Feature extraction

This stage examines the face, fingerprint, and iris as the three biometric features. It was determined that local geometric features may detect certain biometric characteristics. Because local binary pattern (LBP) features are frequently employed in modern research, they were used in this study to represent biometric photos. The feature extraction technique used in computer vision is LBP [18]. The window under consideration is divided into cells, and each pixel is compared with each of its eight neighbors to show the value relationship between a central pixel and its surrounding pixels, as shown in Fig.3. By comparing each pixel, p, to its neighbors, the LBP code is calculated, with a value of 1 being given if '*x*' is greater than or equal to '*p*.' This procedure was repeated for the entire image to create an LBP feature vector. Write "0" if the value of the center pixel is greater than that of its neighbor. If not, type "1”. LBP Characteristics [19]. This approach provided a computational example. The LBP is calculated by translating the binary sequences into decimal values for the selected window and then thresholding the 3 × 3 neighboring pixels of the center pixel with respect to the value of the center pixel. LBP histograms showing the total number of transitions from 0 to 1 for each pixel's eight neighbors were produced using the decimal values of each biometric image. The following equation can be used to determine LBP [20]:

$$LBP = \sum_{i=1}^{P} \sum_{j=1}^{P} (g_i - g_j) \cdot \sigma(x_i - x_j) \quad \text{-------------}(1)$$

where:

LBP is the LBP value of central pixel xi in a cell of size *P×P.*

g_i is the intensity value of the neighboring pixel with index i in a circular neighborhood of radius *R*.

σ is a step function that controls quantization of the method.

P is the number of sampling points on a circle of radius *R.*

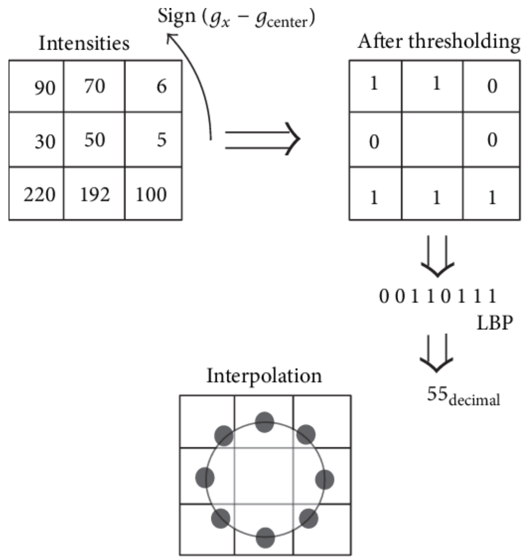


Fig .3- LBP calculation. [19]

3.4 Feature selection (optimization)

Recently, metaheuristic optimization algorithms have been used in many studies. Consequently, in this research, metaheuristic optimization algorithms, such as Particle Swarm Optimization, Genetic Algorithm and Ant Colony Optimization, were implemented. Based on feature selection(optimization)methods, features that are more marked are selected, which helps in building a good classifier model [21]. The acquired optimal features are forwarded as inputs to the classifier algorithm.

3.4.1 Genetic Algorithm

Genetic Algorithms (GA): are heuristic optimization strategies that imitate the evolutionary process in nature. These are a series of iterative processes that employ genetic operators, such as crossover and mutation, to change each population of chromosomes to produce a new population. The answer to this issue is represented by a chromosome, which is a series of bits. Only two possible values (0 or 1) corresponding to various solutions are allowed for each bit [22]. When two chromosomes are randomly chosen from an existing population, and their bits are combined to form a new chromosome, the process is known as crossover. The process of mutation involves randomly changing one chromosomal bit to a different value, which might increase population diversity [23].

Fitness function evaluation measures the quality of a chromosome by comparing it with other chromosomes in the same generation. The fitness function evaluation usually uses an objective function that reflects the goal of the problem, such as minimizing costs or maximizing profits. Fig .4 shows the five essential steps in the GA: chromosome encoding [24], fitness function evaluation, selection of the chromosome strategy, and conditions to stop the GA. The GA population chromosomes were strings of bits. GA selects a limited binary population in a manner similar to natural human evolution. An important step in the GA evaluation is the selection of the fitness function. In this work the fitness function of the population chromosomes is evaluated using KNN classifier error rate [25] [26]. Similar to other parametric methods such as regression, the K-nearest neighbor (K-NN) algorithm is not dependent on a particular equation. Instead, it takes the following course of action.

1)Measure the separation between each training set instance and test instance. Although Manhattan and Minkowski can also be used, Euclidean is the most popular distance unit.

2)Find the K closest examples by sorting the distances.

3)Compile categories for these occurrences.

4)The category that appeared most frequently in the test case was the one that was predicted.

It can be stated as follows in terms of conditional probability: [27]

$$P(Y = j|X = x_0) = \frac{1}{k} \sum_{i \in N_0} I(y_i = j) \quad \text{---------------(27)}$$

Where:

• Y is the output variable (class/category)

• j is a specific class

• X is the input instance

• x0 is a specific instance

• k is the number of nearest neighbors

• N0 is the set of k nearest neighbors to x0

• I () is an indicator function that equals one when yi=j; otherwise, it equals zero.

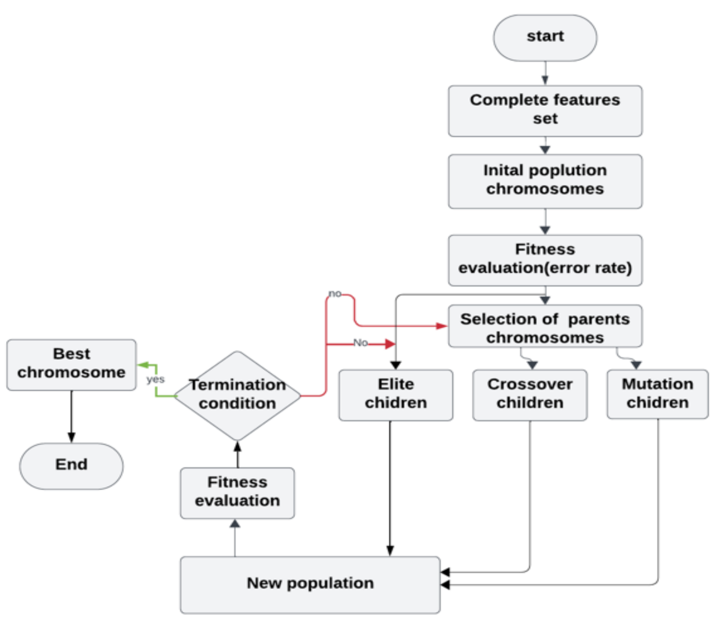


Fig .4 - the GA algorithm flowchart.

3.4.2 Particle Swarm Optimization (PSO)

A metaheuristic method called Particle Swarm Optimization (PSO) is motivated by the flocking of swarms of birds or other animals to a certain area to accomplish objectives in a multidimensional space. In essence, a swarm is a population of particles or individuals, and this program searches by utilizing only one. Each iteration updates these particles such that the final result becomes closer [28] [29]. Depending on these two essential factors, each particle modifies the search direction.

1. The particle's p-best— the best prior experience—is the first consideration.

2. The g-best particle, or the one with the best experience among all others in the swarm.

Each particle is directed by these two parameters to the regions of the search space that have previously produced successful results, causing a collective movement towards optimal or nearly ideal solutions.

The PSO method selects the best characteristics. The effectiveness and efficiency of the algorithm depends on this choice. Numerous PSO-related topics have been the subject of recent research, such as the impact of parameter tuning on system behavior, design of stopping criteria for predicting solution dependability and reducing computational cost, and creation of constraint-handling methods [30]. PSO has also been used in Artificial Neural Network (ANN) applications [31], and the PSO parameters have been optimized for better outcomes. Fig. 5 depicts the PSO algorithm process for selecting the best characteristics [32].

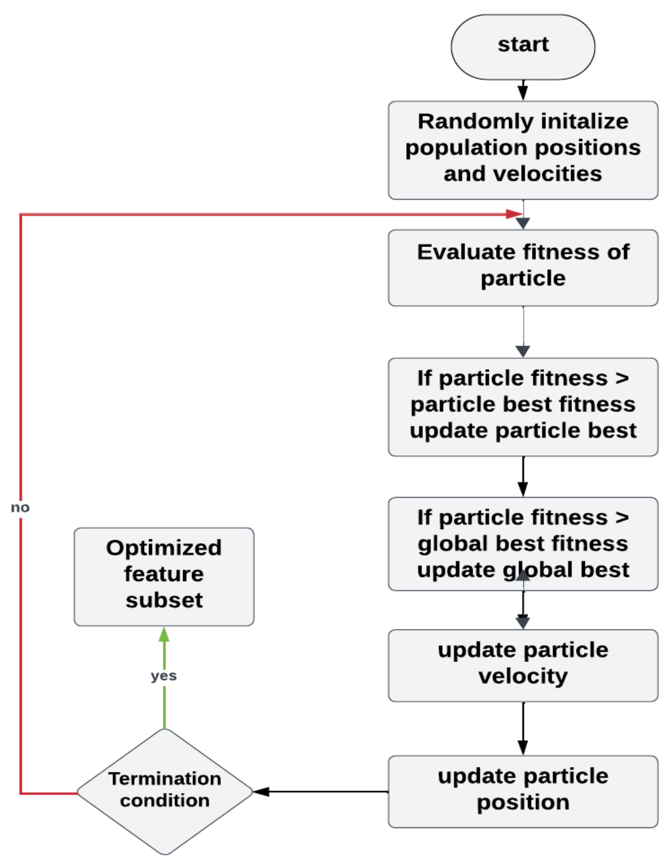


Fig .5 - the PSO algorithm flowchart. [32]

3.4.3 Ant Colony Optimization (ACO)

A metaheuristic called Ant Colony Optimization (ACO) was developed after observing how ant colonies forage. Marco Dorigo initially presented it in the 1990s. Ants are eusocial insects that prioritize the survival of individual species.

They use pheromones, touch, and sound to interact with one another. Pheromones are organic chemical substances released by ants that cause other individuals of the same species to act socially [33].

The fundamental idea behind the ACO is to watch how ants leave their nests and travel as little a distance as possible in the quest for food. The ants initially began to travel randomly to look for food near their nests. Multiple paths leading from the nest to a food source become available because of this random search. Now, ants bring some of the food back with the requisite signal concentration on their return trip, depending on the quality and amount of food. The likelihood that subsequent ants would choose a particular route based on these scent trials would serve as a guiding element for their food source. Evidently, both the concentration and velocity of pheromone evaporation play a role in determining this probability [34].

Research on ACO has made tremendous progress in recent years. For example, the Focused ACO (FACO) innovative variant offers a technique for managing the number of variations between a freshly created and chosen prior solution. Consequently, the search process becomes more narrowly focused, making it possible to uncover improvements while maintaining the caliber of the current solution [35]. Complex combinatorial optimization issues, including the problem of the traveling salesman (TSP) and the vehicle routing problem (VRP), have been successfully solved using ACO. The ACO procedure for feature selection is shown in Fig. 6. [36].

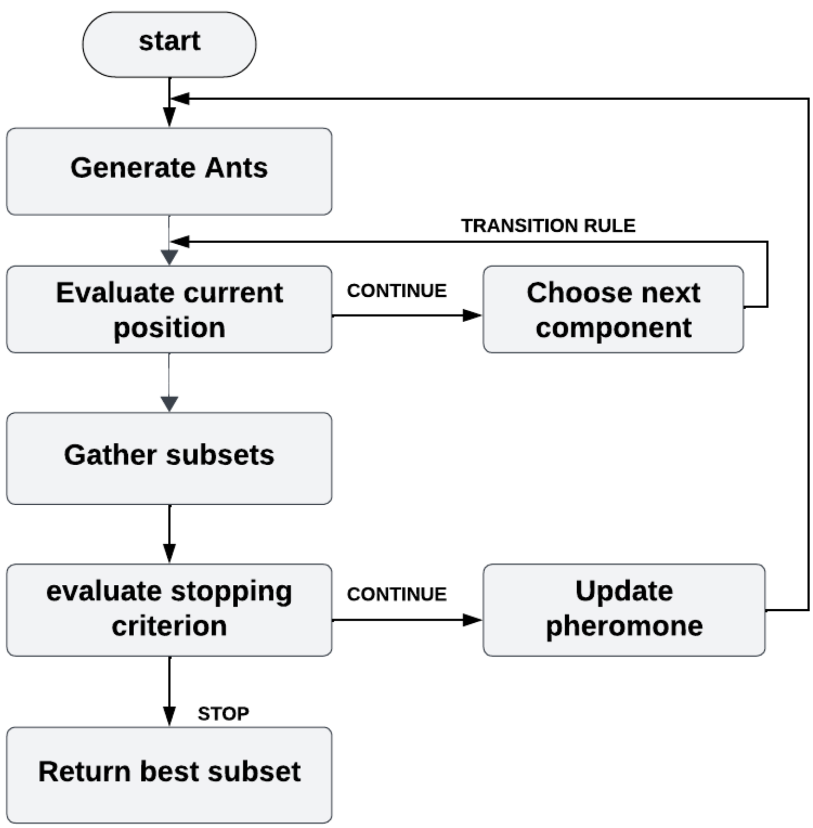


Fig .6 - the ACO algorithm flowchart

3.5. Feature fusion

Feature level fusion refers to methods that combine various features obtained from the same or separate input data. This can be equivalent to numerous feature vectors for the same biometric type. It could also correspond to features extracted from different modalities, such as fingerprints, faces, and iris images [37]. Feature-level fusion joins different characterizations to generate a single representation of a given individual. Consequently, a single feature vector was fed to the classifier algorithm [38].

3.6 Classification

The supervised machine learning algorithm, known as Support Vector Machines (SVM), works in an n-dimensional space, where n is the number of features in the input data. In this high-dimensional space, each feature is plotted as a point. The SVM method divides data points into separate categories by identifying the best hyperplane [39]. This hyperplane is defined as "optimal" when the distance between the closest data points in each class is maximized. SVM is effective in high-dimensional areas and is flexible to outliers owing to this property [40].

The kernel trick is a method used by the SVM when the data cannot be split linearly. Using this method, the data points are transformed into a higher-dimensional space, where they can be linearly separated. Each data point is mapped to a separate feature space using the kernel function that is applied to it [41].

Then, by minimizing the cost function, which is sometimes referred to as the loss function, a perfect hyperplane is found. The effectiveness of the hyperplane class separation was evaluated using this function. Different loss functions may be required for various types of issues, including regression (continuous output), multiclass classification (more than two classes), and binary classification (two classes) [42].

In addition, the gamma parameter, kernel type, and kernel parameters were used by the SVM algorithm to determine its behavior. These variables affect the kernel function's sensitivity to outliers or noise as well as the way it fits the data., as shown in Fig .7 [43]

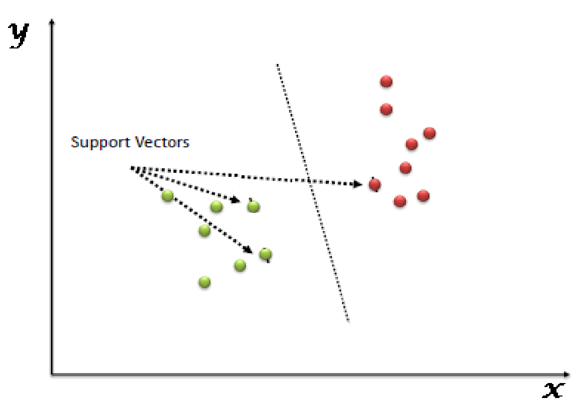


Fig.7- SVM algorithm. [43]

4. Experimental results

In this paper, we propose a multibiometric recognition system that utilizes the SDUMLA-HMT dataset, which comprises 1060 iris images, 8904 face images, and 25,440 fingerprint images. The images for each class in the SDUMLA-HMT dataset were divided into training, validation, and testing sets at a 60:20:20 ratio. Specifically, 60% of the images were used for training, 20% for validation, and 20% for testing. The images from the dataset were organized into three separate folders for training, validation, and testing. Each folder contained samples from each subject.

Evaluating these results is a crucial step in assessing the effectiveness of the proposed recognition system. In this study, three evaluation metrics were used: accuracy, precision, and recall. Accuracy was defined as the ratio of correctly classified subjects to the total number of subjects.

$$Acc = \frac{TP + TN}{TP + FP + TN + FN} \text{-------------------[44]}$$

The recall can be defined as the ratio between the correctly classified positive samples and the total fraction of positive samples.

$$Sn = \frac{TP}{TP + FN} \quad \text{----------------------------[45]}$$

Precision refers to the number of positive cases detected and positive cases.

$$recision = \frac{TP}{TP + FP} \text{-------------------------[46]}$$

In this study, the GA, PSO, and ACO optimization metaheuristics were used, and their initial parameters are recorded in table 1,2,3 respectively. These parameters were manually selected and tested to obtain the best performance results.

Table 1- GA parameters

The parameter	**The initial value**
Number of generations	10
Crossover probability	0.7
Mutation probability	0.1
Size of population	10

Table 2 - PSO parameters

The parameter	**The initial value**
Personal learning factor	2
Global learning factor	2
Weight of inertia	0.7
Size of swarm	20

Table 3- ACO parameters

The parameter	The initial value
Number of ants	10
Beta	1
Alpha	1
Rho	0.05

Tables (4) – (7) record the results of applying the proposed system to the iris, face, and fingerprint biometric individually and multimodal models, respectively. The tables describe the identification accuracy, precision, and recall findings from the experiments conducted. The findings show that compared to unimodal models, the multimodal biometric model achieved higher accuracy rates. In addition, the PSO method provided better results than ACO and GA. This demonstrates that multimodal biometrics offers a highly effective technique for increasing the accuracy rates of a biometric system, as initially intended.

Table 4 -Iris biometric results

Iris Biometric	PSO	AG	ACO
Accuracy	87.64%	80.07%	72.65%
Precision	86.52%	79.05%	71.53%
Recall	87.28%	79.75%	72.18%

Table 5 - Face biometric results

Face Biometric	PSO	AG	ACO
Accuracy	84.53%	80.04%	78.73%
Precision	83.13%	79.26%	75.55%
Recall	84.12%	79.66%	72.14%

Table 6 - Fingerprint biometric results

Fingerprint Biometric	PSO	AG	ACO
Accuracy	81.63%	78.13%	77.19%
Precision	80.19%	77.44%	76.38%
Recall	81.21%	77.87%	76.91%

Table 7 – Multi-biometric results

Iris, face and fingerprint Biometric	PSO	AG	ACO
Accuracy	99.4%	96.05%	89.17%
Precision	98.42%	95.25%	83.13%
Recall	99.22%	94.19%	84.12%

5- Results discussion

In the proposed system, the identification process is enhanced to address security problems when a single biometric is used. Table 8 lists the accuracy results of the proposed system performance compared with state-of-the-art systems. The table illustrates the two previous studies that used the SDUMLA-HMT dataset. These two studies [37] [38] produced a multimodal system based on the use of a deep learning algorithm, which is currently the most famous artificial intelligence algorithm for recognition and classification.

The result of the proposed method is markedly higher than that of [37], which uses score-level fusion to fuse (iris, face, finger vein, and palm print). Another study [38] employed multilevel feature fusion for signature and fingerprint biometrics. Both of these studies used a CNN algorithm for identification, which is a complex artificial intelligence algorithm for implementation. In contrast, the proposed system is more accurate and easier to implement.

Table (8) Compare with the state of art research results

References	Traits	Accuracy
[15]	iris, face, finger vein and palm print	94.00%
[26]	fingerprint - Signature	93.33%
Our proposed model	face, iris and fingerprint	99.4%

6- Conclusion

The multimodal biometric system (facial, iris, and fingerprint) presented in this study uses metaheuristic optimization methods to select the best characteristics for biometric image reconstruction. This study is the first to investigate the use of optimization algorithms for multimodal biometric recognition. The system achieved excellent accuracy by combining the features of the three biometrics at the attribute level. The system achieved the best performance of 99.4% when employing the Particle Swarm Optimization (PSO) algorithm for feature selection, according to the testing results on the SDUMLA-HMT dataset. Future research on this subject may examine the system's resistance to various threats and noises that might interfere with biometric information. This makes it easier to assess how effectively the system can withstand malicious inputs and safeguard biometric data. The system can also be compared to other innovative multimodal biometric systems in the future to determine its benefits and drawbacks.

References

[1] K. Nandakumar, A. K. Jain, and A. Ross, *Introduction to Biometrics*. Springer, 2011. [Online]. Available: https://doi.org/10.1007/978-0-387-77326-1

[2] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognit. Lett.*, vol. 79, pp. 80-105, 2016.

[3] S. Vishwas and L. D. Resolution, *E-Handbook Sabka Vishwas (Legacy Dispute Resolution) Scheme*, 2019.

[4] A. Ross, "Biometrics: An Overview," in *Handbook of Biometrics for Forensic Science*, M. Tistarelli and C. Champod, Eds., Cham, Switzerland: Springer, 2019.

[5] A. BcH.N. Prakash, "Multimodal Biometric Recognition System Using Face and Finger Vein Biometric Traits with Feature and Decision Level Fusion Techniques," *International Journal of Computer Theory and Engineering*, vol. 13(4), pp. 123-128, Sep. 2021.

[6] M. Soltane, S. Bakhti, and M. Soltane, "Multi-modal biometric authentication: Concept issues and application strategies," *International Journal of Computer Theory and Engineering*, vol. 48(3), pp. 23-60, 2012.

[7] M. O. Oloyede and G. P. Hancke, "Unimodal and Multimodal Biometric Sensing Systems: A Review," *IEEE Access*, vol. 4, pp. 7532-7555, 2016.

[8] B. Ammour et al., "Face–iris multimodal biometric identification system," *Electronics*, vol. 9(1), p. 85, Jan. 2020.

[9] H. Zhang and Z. Yang, "Biometric Authentication and Correlation Analysis Based on CNN-SRU Hybrid Neural Network Model," *Computational Intelligence and Neuroscience*, vol. 2023, Article ID 8389193.

[10] D. Chang et al., "BIOFUSE: A framework for multi-biometric fusion on bio cryptosystem level," *Information Sciences*, vol. 546, pp. 481-511, 2021.

[11] M. Garg et al., "A novel feature biometric fusion approach for iris, speech and signature," *Computer Methods in Material Science*, vol. 20(2), pp. 101-109, 2020.

[12] S.Sengar et al., "Multimodal biometric authentication system using deep learning method," in *2021 International Conference on Circuits, Controls and Communications (CCUBE)*, pp:1-6.

[13] R.Vinothkanna et al., "A multimodal biometric approach for the recognition of finger print, palm print and hand vein using fuzzy vault," *International Journal of Biometrics*, vol:12(3), pp:233–250.

[14] T.Kumar et al., "An Improved Biometric Fusion System of Fingerprint and Face using Whale Optimization," in *2021 International Conference on Communication Computing and Electronics Systems (ICCCES)*.

[15] B.O.Mohammed et al., "New feature-level algorithm for a face-fingerprint integral multi-biometrics identification system," *UHD Journal of Science and Technology*, vol:6(1), pp:12–20.

[16] Y. Yin, L. Liu, and X. Sun, "SDUMLA-HMT: A multimodal biometric database," in *Proceedings of the 5th International Conference on Biometrics (ICB)*, 2012, pp. 260-268.

[17] J. Fierrez et al., "BiosecurID: a multimodal biometric database," arXiv preprint arXiv:2111.03472, Nov. 2021. [Online]. Available: arXiv.org.

[18] I. Oztel, G. Oztel, and D. Akgun, "A hybrid LBP-DCNN based feature extraction method in YOLO: An application for masked face and social distance detection," *Multimedia Tools and Applications*, vol. 82(1), pp. 1565-1583, 2022.

[19] O. Lahdenoja, J. Poikonen, and M. Laiho, "Towards understanding the formation of uniform local binary patterns," *International Scholarly Research Notices*, vol. 2013, Article ID 429347.

[20] M. A. Rahim et al., "Face recognition using local binary patterns (LBP)," *Global Journal of Computer Science and Technology*, vol. 13(4), pp. 1-6, 2013.

[21] N. Ansari, "A survey on feature selection techniques using evolutionary algorithms," *Iraqi Journal of Science*, vol. 62(8), pp. 2796-2812, 2021.

[22] N. A. K. Hussein and B. Al-Sarray, "Deep learning and machine learning via a genetic algorithm to classify breast cancer DNA data," *Iraqi Journal of Science*, vol. 63(7), pp. 3153-3168, 2022.
[23] S.Katoch et al., "A review on genetic algorithm: past, present, and future," *Multimedia Tools and Applications*, vol:80, pp:8091–8126.
[24] D.Whitley and A.M.Sutton, "Genetic Algorithms — A Survey of Models and Methods," in *Genetic Algorithms: A Comprehensive Introduction*, Springer.
[25] S.Katoch et al., "A review on genetic algorithm: past, present, and future," *International Journal of Computer Science and Information Technology*, vol:8(2), pp:1-10.
[26] K.K.Srinivasan, "Genetic Algorithms | SpringerLink."
[27] P.Wang et al., "Application of K-Nearest Neighbor (KNN) Algorithm for Human Action Recognition," in *2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*.
[28]"Particle Swarm Optimization: A Comprehensive Survey," in *IEEE Access*, vol:10.
[29] A.G.Gad, "Particle Swarm Optimization Algorithm and Its Applications: A Systematic Review," in *Archives of Computational Methods in Engineering*.
[30] "Improvement of Particle Swarm Optimization Focusing on Diversity of the Particle Swarm," in 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 11-14 October 2020. [Online]. Available:
[31] S. Sengupta, S. Basak, and R. A. Peters II, "Particle Swarm Optimization: A survey of historical and recent developments with hybridization perspectives," ARXIV PREPRINT ARXIV:1804.05319, 2018. [Online]. Available:
[32] R. A. Ibrahim et al., "Improved salp swarm algorithm based on particle swarm optimization for feature selection," J. Ambient Intell. Humaniz. Comput., vol. 10, no. 8, pp. 3155–3169, Aug. 2019.
[33] M. Dorigo and G. Di Caro, "Ant colony optimization: a new meta-heuristic," in Proceedings of the 1999 Congress on Evolutionary Computation-CEC99 (Cat. No. 99TH8406), 1999.
[34] M. Dorigo, "Ant colony optimization," IEEE Computational Intelligence Magazine, vol. 1, no. 4, pp. 28-39, Nov. 2006.
[35] "Improving Ant Colony Optimization Efficiency for Solving Combinatorial Optimization Problems," arXiv:2203.02228 [cs.NE], Mar. 2023.
[36] H.R.Kanan et al., "Feature selection using ant colony optimization (ACO): a new method and comparative study in the application of face recognition system." Industrial conference on data mining. Springer, Berlin, Heidelberg, 2007.
[37] T.Vijayakumar, "Synthesis of palm print in feature fusion techniques for multimodal biometric recognition system online signature," J. Innov. Image Process., vol:3(2), pp:131–143.
[38] A.B.Channegowda et al., "Multimodal biometrics of fingerprint and signature recognition using multi-level feature fusion and deep learnin… Indonesian.pdf." 2021.
[39] T.Evgeniou et al., "Support Vector Machines: Theory and Applications," in L.Wang (ed.), Encyclopedia of Machine Learning, vol:1, Springer, Cham, 2019.
[40] S.Saikin et al., "Optimization of Support Vector Machine Method Using Feature Selection to Improve Classification Results." JISA (Jurnal Informatika dan Sains), vol:4(1), pp:1-10.
[41] B.Gaye et al., "Improvement of Support Vector Machine Algorithm in Big Data Background." Mathematical Problems in Engineering, Article ID 5594899.
[42] S.Theodoridis et al., "Support Vector Machines for Classification," in Pattern Recognition, 5th ed., Cambridge, MA, USA: Academic Press, ch:5, pp:211-282.
[43] Y.Zhang, "Support vector machine classification algorithm and its application." International conference on information computing and applications. Springer, Berlin, Heidelberg, 2012.
[44] J.Shreffler et al., Diagnostic Testing Accuracy: Sensitivity, Specificity, Predictive Values and Likelihood Ratios. StatPearls Publishing LLC; 2023.
[45] J.Brownlee, "How to Calculate Precision, Recall, and F-Measure for Imbalanced Classification," Machine Learning Mastery, Jan. 2020.
[46] A.B.Channegowda et al., "Multimodal biometrics of fingerprint and signature recognition using multi-level feature fusion and deep learning," in 2021 11th International Conference on Computing Communication and Networking Technologies (ICCCNT).