Enhancing Human Identification Systems Through Bi-modal Fusion Using Negative Selection Algorithm

[1]Monsurat O. Balogun, [2]Bilkisu Jimade-Ojuolape & [3]Latifat A. Odeniyi

[1]Department of Electrical and Computer Engineering, Kwara State University, Malete, Ilorin, Kwara State, Nigeria.
[2]Department of Electrical and Computer Engineering, Kwara State University, Malete, Ilorin, Kwara State, Nigeria..
[3]Department of Mathematical and Computing Scienced, Koladaisi University, Ibadan, Oyo State, Nigeria.

: Monsurat.balogun@kwasu.edu.ng; + (234) 8035196151

Received: 22.10.2023 **Revised**: 06.02.2024 **Accepted**: 13.02.2024 **Published**: 27.02.2024

Abstract:
The Negative Selection Algorithm (NSA) is a computational technique inspired by the human immune system and widely used in various fields like intrusion detection, network security, data mining, and pattern recognition. However, its effectiveness in human identification has not been thoroughly explored. This study focuses on utilizing NSA for human image classification, specifically in a bi-modal system combining physiological traits (faces and fingerprints) and behavioral traits (signatures and voices), as well as a uni-modal system using all features. The research collected 2400 images from 200 individuals, pre-processed images, and salient features selected for easy classification. NSA was used for image classification in both bi-modal and uni-modal systems. The results demonstrated NSA's effectiveness, particularly in the bi-modal system. The biometric system that fused behavioral traits exhibited high accuracy, with true positive and true negative rates of 141% and 144%, respectively, and an overall accuracy of 95%. The system is based solely on physiological traits and achieved slightly lower accuracy rates at 89%. Furthermore, among the uni-modal systems, the voice-based system stood out with a true positive rate of 131% and an accuracy of 88.33%. These findings emphasize the advantages of combining different biometric traits, showcasing the potential for increased accuracy in identification systems. The study highlights NSA's role in enhancing classification accuracy, suggesting the developed biometric systems could significantly improve the performance and reliability of various integrated identification systems.

Keywords: *Biometrics, Feature Fusion, Feature Extraction, Identification, Immune System, Negative Selection*

I. INTRODUCTION

The Negative Selection Algorithm (NSA), also known as Artificial Immune Systems, has emerged as a significant technique within Immunological Computation. It has gained recognition for its ability to mimic the human immune system's negative selection process, which plays a vital role in distinguishing between self and non-self-entities [1]. The NSA has proven its potential as a powerful computational tool by harnessing this biological inspiration. It exhibits the capacity to identify and eliminate undesirable entities while preserving and selecting the most suitable ones, and this has significantly contributed to its effectiveness as an efficient problem-solving approach. Several studies have considered implementing the NSA algorithm in anomalous and fault detection. Ji and Dasgupta [2] applied NSA in fault and anomaly detection. Studies [1] and [3] used NSA in Fault detection of aircraft control system. De et al. [4] employed NSA to conduct sensitivity analysis of the negative selection algorithm applied to anomaly identification in builds. Hosseini et al. [5] engaged NSA alongside other human-inspired algorithms for Botnet detection purpose. Jin and Ming [6]used NSA to construct self-set for identity based in fault detection. Mousavi et al.[7] used NSA for dengue outbreak detection. Pamukov and Poulkov [8] deployed multiple negative selection algorithms to improve detection error rates in IoT intrusion detection systems. Ren et al. [9] developed a novel fault diagnosis method based on improved negative selection algorithms.

However, only a few studies have employed its one-class identification capability in human identification. Therefore, the performance of NSA in biometric image classification is evaluated in this study, considering the influences of human identification in various activities. Human identification is the process of recognizing and verifying a person's identity based on their biological and behavioral characteristics [10]. Among the different methods and technologies that can be used for human identification is biometric identification. Biometric identification is the use of body measurements and calculations of human characteristics, such as fingerprints, iris, voice, and so on, to identify and authenticate a person [11]. Biometric identifiers are unique and reliable features of a person’s body and behavior that can be measured and compared with a database. Biometric identification systems are widely used in security, law enforcement, banking, and immigration.

Biometric is the process of using the inherent properties of human beings in identity creation [12]. The inherent properties can be physiological (face, fingerprint, iris, palm vain) or behavioral (signature, voice, gait). One valuable tool used in decision making is identity, which, if not well established, can lead to so much misinformation [13]. Identity is a characteristic that determines who or what a person or thing is and there are two major ways of creating identity: the conventional/traditional way and biometric way.

The conventional way involves using the information possessed by a person such as name, home address, identification number, identification card and so on in identity creation, while biometric uses measurable properties of human in creating identity [14]. The formal has been prone to many errors such as forgery, spoofing, inaccuracy and so on. From research biometrics are the most secure and accurate mode of identity creation.

Biometric involves measurement of unique physiological or behavioral human characteristics. The measured values can then be used for identity creation in digital realms. Biometric has been described as the most reliable and suitable means of human identification [15]. Biometric system is a pattern recognition system which identifies a person by determining the authenticity of a specific behavioral or physiological characteristic possessed by the person [16]. Biometric system is of two major types: single-biometric (uni-modal) and multi-biometric (multi-modal). Uni-modal biometric involves using a single biometric evidence/information in creating an identification/authentication system, while multi-modal biometric involves using more than one biometric evidence/information in identity creation [10].

Different types of multi-biometric systems exist, such as multi-instance, multi-algorithms, multi-sample, multi-sensor, multi-modal and hybrid biometric system[17]. Multi-instance involves fusion of evidence from the same biometric characteristic with different object expressions captured at different times. Multi-algorithms involve fusion of biometric evidence of the same biometric trait extracted using different extraction algorithms. Multi-sample is the mixture of multiple of the same samples of a biometric trait capture using one capturing device, while multi-sensor involves mixture of evidence of the same biometric trait captured using different capturing devices. Multi-modal is the process of fussing evidence from two or more biometric traits. Hybrid biometric system is a system that combines two or more of the other types of multi-biometric systems[18].

A bi-modal biometric system combines two biometric traits to overcome the limitations of uni-modal-biometric system [19]. Mostly, uni-modal systems suffer from the limitation of the biometric identifier/trait considered, however, combination of more than one identifier/trait (bi-modal system) allows for check and balance between the benefits and limitations of different identifiers [20]. Hence, this work designed bi-modal biometric systems that combined physiological traits (face and fingerprint) and behavioral traits (signature and voice). Bi-modal biometric system consists of six basic stages: image capturing, image pre-processing, features extraction, features fusion, classification and decision making.

Image capturing is a stage of a biometric system in which the required raw biometric evidence or traits are acquired. This stage is very important because it greatly influences the overall system performance. Image pre-process involves error removal and fine-tuning of the acquired image [21]. Feature extraction involves mining of the useful and salient properties of the pre-processed images. In bi-biometric, feature fusion involves mixture of the salient biometric information/features gathered at the feature extraction stage. Care must be taken at this stage, because if the biometric features are heterogeneous, feature normalization must be carried before fusion [10]. Feature normalization brings all the feature into common domain and helps in preventing a feature from dominating the feature samples [22]. However, if the features are homogeneous such multi-sample or multi-instance system normalization is not necessarily required.

Feature normalization gives all the traits equal chance of contributing during feature fusion [23]. Follows by feature fusion is classification/ image classification. Image classification is the decision-making stage of a biometric system because this is the stage at which the final decision about the identity is made.

II. RELATED STUDIES

Much research has been carried out on improving the performance of biometric identification systems, especially multi-biometric systems. Decision on the best fusion technique and the best fusion level has always been major issues in multi-biometric systems. Features fusion can be carried out at different stages in multi-biometric system ranges from sensor level, feature level, match score and abstract/decision level fusion. The best fusion level's choice depends on factors such as the level of accuracy required from the system, nature of the considered biometric traits, size of the data and fusion technique used in a particular system. To improve the performance of multi-biometric systems, many researchers have employed different fusion techniques at different levels of fusion as reviewed below. Hosseini and Seilani [24] used Negative Selection in anomaly process detection where the anomaly is non-self in the system. The authors present a new combined technique for anomaly process detection. The combined technique is a unification of both negative selection and classification algorithm. CICIDS 2017 and NSL-KDD dataset with different sets of features and the same number of detectors are used. The WEKA tool classification performed a correlation-based feature selection on the dataset. The technique was evaluated using machine learning algorithms such as: logistic regression, random forest, decision tree and K-neighbors and it was discovered that NSA outperformed other algorithms.

Zhang and Xiao [25] proposed a real-valued negative selection algorithm based on clonal selection. Firstly, the algorithm analyzes the space distribution of the self-set and gets the set of outlier selves and several classification clusters. The algorithm considers centers of clusters as antigens, randomly generates initial immune cell population in the qualified range and executes the clonal selection algorithm. Afterwards, the algorithm changes the limited range to continue the iteration until the non-self-space coverage rate meets expectations. After the algorithm terminates, mature detector set, and boundary self-set are obtained. Arteaga-Falconi et al. [26]proposed a multimodal biometric approach based on ECG and Fingerprint to secure the interaction between "things" and people. The work enhances the advantages of both biometric methods while minimizing their weaknesses. SVM was used as classifier for ECG and minutiae extractor and matcher from NBIS were employed for fingerprint technique. The ECG and Fingerprint authentication results were fused at the decision level to distinguish between genuine users and impostors. The results obtained show that this work presents an improvement in terms of EER (Equal Error Rate) compared to existing work. Okokpujie et al. [27] and Joseph [28] proposed a secure and automated bimodal voting system. Xue and Zhou [29] presented new techniques for designing a simple and reliable multi-featured biometric system based on a single trait source. One-to-one relationship between the feature's edge and its associated angle is utilized after extracting the contrast feature using the gray-level co-occurring matrix (GLCM) method. The classifying stage is modified to process one-dimensional vectors rather than the whole feature's template. For comparison purposes, the performance of the three biometric systems was based on 170 subjects taken from four facial databases. Comparisons are made using three error distance measurements.

Srivastava et al. [30] developed a combination biometric framework in which principal component analysis (PCA) and linear binary pattern (LBP) are applied on both face and palm prints to generate a unique score that is used to authenticate the human. For validation of the framework two different databases, ORL (Olivetti Research Laboratory) and PolyU (Hong Kong Polytechnic University) are used. The framework achieved an accuracy of 99.8%, which is far better as compared to the unimodal system.

Safavipour et al, [31]face and Palm-print traits were fused at feature level in a multi-biometric system. Features were fused at feature level using the improved K-medoids clustering algorithm and isomorphic graph. The set of n-invariant features were partitioned into K-clusters using pertaining around method (PAM). Most feasible pair of graphs were examined using iterative relaxation algorithm from all isomorphic graphs for a pair of related face and palm print images. Experimental results obtained showed that the K-medoids partitioning algorithm improved the system performance with 0.0% FAR and 99.5% recognition rate. Balogun et al, [10] developed a multi-biometric system that fused features of face, fingerprint, iris, signature, and voice. Over 6000 biometric evidence used in the work were collected from black people and two different biometric systems were developed (uni-modal of each trait and a multi-modal that combined all the traits). Features were extracted using Principal Component Analysis (PCA) and the extracted features were fused at feature level using Weighted Average Method (WAM) in the multi-modal system, While Optimized Negative Selection Algorithm was used as classifier. Recognition accuracy of the two biometric systems developed were compared and it was discovered that, the multi-modal system has the best recognition accuracy by producing recognition accuracy of 98.33% at 0.98 recognition threshold, compared to those the uni-modal systems that are 90.33%, 89.67%, 89.00%, 88.33% and 87.67%, at the same recognition threshold, respectively.

Herbadji et al. [32] combined three biometric traits of face, palm print and gait. Features were selected using Geometry preserving projections (GPP) algorithm. GPP performs well in class discrimination and retains the intra-modal variation within similar classes. Each biometric trait was trained in sub-space learning using GPP and then the classification was done in the low-dimensional space. Two data arrays named YALE-HKPU-USF and FERET-HKPU-USF were built. The recognition rate obtained using kernel GPP (KGPP) was 90.22% and 93.67 for the YALE-HKPU-USF and FERET-HKPU-USF datasets. [28] fused the features of face and palm print at feature level using PCA and ICA with the Neural Network and support vector machine as the classifier. The result of the bi-modal biometric system was compared with the uni-modal face and palm print biometric systems. It was found out that the performance is significantly improved in the case of feature fusion using ICA by obtaining a favorable result with a 99.17% recognition accuracy using samples collected from 40 people. The limitation of the work is that limited data were considered. Xue and Zhou [29] presented a multi-modal biometric system that combined iris and signature features. User-score-based weighing technique was used to integrate the features of irises and signatures. The weights were applied in depicting the benefits of match score output produced by each biometric attribute. The system produced significantly low FRR of 0.08% and FAR of 0.01%.

Al-sellami et al, [33] designed a system that fused hand geometry and palm-print features. Features were extracted using Discrete Wavelet Transform and classification was done using Support Vector Machine (SVM). Features were fused at match score level. The experiment was able to achieve GAR of 99.47% and FAR of 0% using an existing GPDS database. The limitation of the work was that the experiment was performed on if large data set were used to experiment with the developed system, the accuracy might drastically reduce. Medjahed et al. [34] designed a multimodal biometric system that combined voice, face, finger, and palm features collected from 30 individuals using BOLYBIO datasets. Five instances of data collection were used for each biometrics (multi-instance), four of which were used for training and one for testing. The single voting scheme was used to combine the single trait at the output level. The user is identified if most individuals' modalities vote for the identity, otherwise it is rejected. The notion is since the weak classifier pave way for the powerful classifiers to achieve high performance in terms of both FAR and FRR, even if the best performance is not altered in the single modality system. Evaluations of the result showed that the multi-modal system based on voting scheme at the output level produced the lowest False Acceptance Rate of 1.23% and False Rejection Rate of 0.8%.

Jiang et al. [35] developed a system that is capable of fusing selected few faces with minimum Euclidean distance with finger veins at score level fusion. A low-resolution web camera was used to capture face images and HITACHI finger veins device for finger veins images. The face and finger veins data were collected from 35 CAIRO staffs and students and the system was simulated in C# environment. Both faces and finger veins were extracted using Linear Discriminant Analysis (LDA). The evaluation of the results showed that a low FAR of 0.000026 and high GAR of 97.4% were achieved. The system was tested using a small database which was responsible for the high GAR value gotten. Alay and Al-Baity [36] fused the features of iris, fingerprint, face, and palm-print in a multi-biometric system. Fingerprint samples were collected from a college, irises are from CASIA database, while face and palm geometry are from standard databases. Features were fused at feature level using convolution theorem. The resulting feature vectors were multiplied to obtain the final fused multi-modal template. The final input patterns were classified using probabilistic neural network (PNN) and radial basis function (RBF). Adaptive Cascade based on the principles of mean and variance values was used in comparing the query features with the existing database for identification purposes. The verification phase was based on back- propagation neural network (BPNN) to classify the query data into Genuine/imposter. The experiment produced the following results: 2% FAR, 1.2% FRR and GAR of 98.8. The experiment was conducted using 500 input images, 400 out of which were used for training and the remaining 100 were used for testing. It was observed that the results were gotten from heterogeneous data collection, therefore, the high performance is perceived to be unrealistic.

Hence, in this work, two bi-modal biometric systems were developed: a bi-modal biometric system that combined face and fingerprint (physiological traits) and a bi-modal biometric system that combined signature and voice (behavioral traits). To validate the performance of the two systems, their recognition accuracies based on True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN), False Acceptance Rate (FAR), False Rejection Rate (FRR) and Accuracy were compared with those of the single biometric systems of face, fingerprint, signature, and voice. Presented in Table 1 is the summary of the review of past related works

Table 1: Summary of Related Works

S/N	Author/s names and date	Methodology	Result	Limitation
1	Hosseini et al., (2021)	The authors presented a new combined technique for anomaly process detection, which is a unification of both negative selection and classification algorithms. CICIDS 2017 and NSL-KDD dataset were used.	NSA outperformed other algorithms.	Controlled environment datasets were used.
2	Johnson and Davis. (2019)	Authors proposed an innovative approach that combines the negative selection algorithm with a clonal selection mechanism. Through the evaluations of benchmark datasets.	Performance analysis of the algorithms on complex pattern recognition problems.	Few datasets were considered
3	Anderson and Wilson. (2018)	Developed a method that utilizes the Negative Selection Algorithm (NSA) to detect abnormal behavior in control systems.	The anomalous Detection rate of the was more 88% accurate.	Limited instances were considered.
4	Thompson and Brown, (2020)	Proposed an approach that employs the negative selection algorithm for fault and disturbance detection in power system measurements.	The algorithms showcased a potential improvement in power system reliability.	The performance of the algorithm was not really validated.
5	Forrest *et al,* (1994)	Fusion of Face and Palm-print traits were fused at feature level. Features were fused at feature level using the improved K-medoids clustering algorithm and isomorphic graph.	The evaluation of the system produced 0.0% FAR and 99.5% recognition rate	Limited number of datasets were used.
6	Balogun *et al,* (2023)	Developed a multi-biometric system that fused features of face, fingerprint, iris, signature, and voice.	The multi-modal system has the highest recognition value of 98.33% at 0.98 threshold.	Data used are non-homogeneous.
7	Nulu et al, (2014)	The authors combined three biometric traits of face, palm print and gait. named YALE-HKPU-USF and FERET-HKPU-USF were built.	GPP (KGPP) was 90.22% and 93.67 for the YALE-HKPU-USF and FERET.	Datasets from different sources were used.
8	Falohun *et al,* (2016)	The work fused the features of face and palm print at feature level using PCA and ICA with the Neural Network and support vector machine as the classifier.	ICA obtained a favorable result with 99.17% recognition.	Limited data were considered.

9	Viriri and Tapamo (2012)	Presented a multi-modal biometric system that combined iris and signature features. User-score-based weighing technique was used to integrate the features of irises and signatures.	The system produced significantly low FRR of 0.08% and FAR of 0.01%.	Weak integration methods were employed.
10	Kounoudes *et al,* (2008)	Designed a system that fused hand geometry and palm-print features.	The GAR of 99.47% and FAR of 0%.	The experiment was performed on a small dataset. .
11	Zhang *et al,* (2008)	Designed a multimodal biometric system that combined voice, face, finger, and palm features collected from 30 individuals using BOLYBIO datasets.	False Acceptance Rate of 1.23% and False Rejection Rate of 0.8%.	Limited datasets were used
12	Khan et al, (2011)	Developed a system that is capable of fusing selected few faces with minimum Euclidean distance with finger veins at score level fusion.	The results showed that a low FAR of 0.000026 and high GAR of 97.4% were achieved	The system was tested using a small database.
13	Gawande and Hajari (2013)	Fused the features of iris, fingerprint, face, and palm-print in a multi-biometric system.	The experimental results are: 2% FAR, 1.2% FRR and GAR of 98.8.	Heterogeneous data was used. Hence, the high performance is perceived to be unrealistic.

III. METHODOLOGY

Six (6) different biometric systems were developed in this research, which include: a bi-modal biometric system that combined face and fingerprint (physiological traits), a bi-modal biometric system that combined signature and voice (behavioral traits) and uni-modal of each of the biometric trait. The developed biometric systems were applied for identification purposes. Classification accuracy of the systems was compared based on True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN), False Acceptance Rate (FAR), False Rejection Rate (FRR) and Accuracy.

The biometric traits considered in this work are face and fingerprint (physiological traits) and voice and signature (behavioral traits). Total number of two thousand four hundred (2400) biometric formation of faces, fingerprints, signatures, and voices were acquired. Biometric traits were captured using appropriate capturing devices. Faces were captured using CMITECH face and iris camera, fingerprints were captured using digital personnel fingerprint capturing device, signatures were captured using Topaz T and voices were recorded using android phone voice recorder. Devices were located close to each other for easy access by the users.

Images were pre-processed using histogram equalization. Image preprocessing involves error elimination, pattern localization and detection of salient properties of images. Images of face, fingerprint and signature were first converted to grey scale then histogram equalization, image cropping and binarization. Voices went through pre-processing stages such analog-to-digital conversion, silence detection, pre-emphasis, and windowing.

Following image pre-processing is feature extraction using principal component analysis (PCA), the choice of PCA is due to its ability to extract the best features that can be used to represent image in digital realms without altering the image quality [37]. Selected features from the physiological traits (face and fingerprint) were fused at feature level using weighted average method. The behavioral features (signature and voice) were also fused at feature level using the same fusion method. However, due to the heterogeneous nature of the biometric traits considered, selected features were normalized before fusion using min-max normalization technique algorithm 1 illustrates the min-max normalization steps, while formula representation of the algorithm is shown in Equation 9.

3.1 PCA Steps for Feature Extraction

Assuming 200 images of any of the modalities considered. Using fingerprints as an example, each of which are 150*150 pixels. Essentially, this means each image of fingerprints and all other traits is represented by 22500 numbers (dimensions).

With N-samples of any of the considered traits for instance, fingerprint images,

The mean vector was calculated as follows:

$$\bar{s} = \frac{s_1 + s_2 + s_3 \ldots\ldots\ldots\ldots\ldots + s_N}{N} \quad (1)$$

For every image vector the mean adjusted vector was computed using:

$$\bar{s}_N = (s_i - \bar{s}) \quad (2)$$

All the mean adjusted vectors were put together to form the mean adjusted matrix:

$$S_{mean} = (\bar{s}_i - \bar{s}_N) \quad (3)$$

Therefore, the covariance of $(150 * 150)$ equivalent to $(i * j)$ matrix:

$$Cov_{i,j} = (s_i - \bar{s}).(s_j - \bar{s}) \quad (4)$$

where,
$\bar{s}$ is the mean vector calculated
s_i is the ith image vector
s_j is the jth image vector
The Eigen values, of the covariance matrix was calculated using Equation 5.

$$det(\lambda I - C) = 0 \quad (5)$$

where,
det is the determinant of the matrix
λ is the Eigen values associated with the matrix
I is the identity matrix
The Eigen vector associated for a given high Eigen value is then calculated using:

$$(\lambda_k I - C) * V_k = 0 \quad (6)$$

where,
λ_k= One of the highest Eigen values kept
I = The identity matrix
C = the covariance matrix
V_k= The Eigen vector
Since, the first 15 high Eigen values are to be picked, then there will be 15 Eigen vectors as well (V_1,……….,V_{15}).
Eigen Vector (EV)= $V_1, \ldots \ldots \ldots \ldots \ldots \ldots .., V_{15}$
The basic vector S_B is calculated as follow:

$$S_B = S_{mean} * EV \quad (7)$$

where, S_B= The basic vector with dimension
s_{mean}= The mean adjusted matrix with dimension
EV = The Eigen vector matrix with dimension
Each sample is then expressed as a linear combination of basic vectors using formula:

$$(15\ numbers) = \left(S_{sample} - \bar{S}\right)^T * S_B \quad (8)$$

where,
S_{sample}= The sample to be represented using basic vector
$\bar{S}$ = The mean adjusted vector with dimension $(15 * 1)$
S_B = The basic vector with dimension $(150 * 150)$
With these steps each image being represented by 22,500 numbers, is now represented by 15 numbers.

Algorithm 1: **Min-max normalization**

Start
Create a vector x that contains selected features of a biometric treat;
Load the minimum absolute value, min(x), in the vector x;
Load the maximum absolute value, max(x), in the vector x;
Generate an empty set of x';
For each x_i, ϵ x,
Calculate the normalized value, x'_i, using the formula:
x'_i = (x_i - min(x)) / (max(x) - min(x));
Add x'_i to the vector x';
End **For**
Return the normalized vector x' as the output;
End.

$$x' = \frac{x - min(x)}{max(x) - min(x)} \quad (9)$$

Where; x is the original binary representation of the image
x' is the normalized value
$Max(x)$ is the maximum weight
$Min\ (x)$ is the minimum weight.

Feature normalization was done to bring all the selected features into common domain for easy fusion. The Weighted Average Method given in Equation 10 was used for feature fusion. Feature fusion involves a mixture of all features extracted from the biometric traits. Algorithm 2 shows the step implementation of Equation 2.

Algorithm 2: **Weighted Average Method**
Start
Initialize variables;
$sum\_scores = 0$
$sum\_weights = 0$
$weighted\_ave = 0$
IF $score = weight$.;
For (i=1; i= n; ++i)
$Sum\_score = \sum_{i=1}^{n} score_i$;
$sum\_weight = \sum_{i=1}^{n} weight_i$;
` $weighted\_score = sum\_score * sum\_weight$;
End For
End IF
$weighted_{ave} = \frac{1}{m}\sum_{i=1}^{n} weighted\_score$;
Return $weighted_{ave}$;
End.

$$weighted_{Ave} = \frac{1}{m}\sum_{i}^{n} weight_i . score_i$$

Where, m is the value used to normalize the score (ranges from 0-1), n is the total number of modalities, $weight_i$ is the weight of each single modality and $score_i$ is the matching score of each single modality.

Classification was done using Negative Selection Algorithm (NSA). The choice of NSA as classifier in this work is because of its ability to proffered solution to computational problems such as computer security, network security and anomalies detection problems to mention but few. NSA imitates the working mechanism of mammalian immune system, in which its major aim is to classify a bit or string of bits' representation of real-world data, terms as features into self (normal) or non-self (anomalous) and the basic idea is to generate a number of detector features that can be used to classify new data or pattern (unseen data) as self or non-self. He et al. [38], NSA carries out its processes in two phases (learning phase and recognition phase).

Learning phase is the stage at which a set of self-features is used in training the algorithm using the negative selection technique, while recognition phase is the phase at which the trained self-feature set is exposed to a set of self and non-self-features for classification purposes. To examine the performance of biometric systems, the system reactions to large number of queries features from both authorized and non-authorized subjects are usually observed. Due to the natural fluctuations and measurement imperfections, the result from such action can never be said to be truly certain, though can be predictable to a certain extent. To deal with the imperfection that may arise because of bias prediction, a particular value can be set by the users, in which match templates that fall within the value are categories as authentic and those below as unauthentic/intruder. This kind of template matches authentication range or value and is referred to as threshold value in biometric systems.

The acceptance and rejection of a template match depends on the match score falling with the reference threshold. Four different affinity threshold values were observed in this research which includes (0.09, 0.36, 0.44 and 0.98). It was observed that the affinity thresholds between 0 to 0.08 produced no significant observation in the performance metrics, also between 0.10 to 0.35 there was no significant difference, as well as between 0.37 to 0.43 and between 0.45 to 0.97. It was found out that the system performs better with greater accuracy when 0.98 was used as threshold value. Hence, 0.98 was used as reference threshold value for all the biometric systems considered in this work. The algorithm for NSA is as shown in Algorithm 3, while Fig. 1 illustrates flowchart of the NSA implementation. Shown in Figs. 2, 3 and 4 are the block diagrams of the developed biometric systems, while Figs. 5 and 6 showed the graphical user interface for the two developed bi-modal biometric systems implemented in MATLAB.

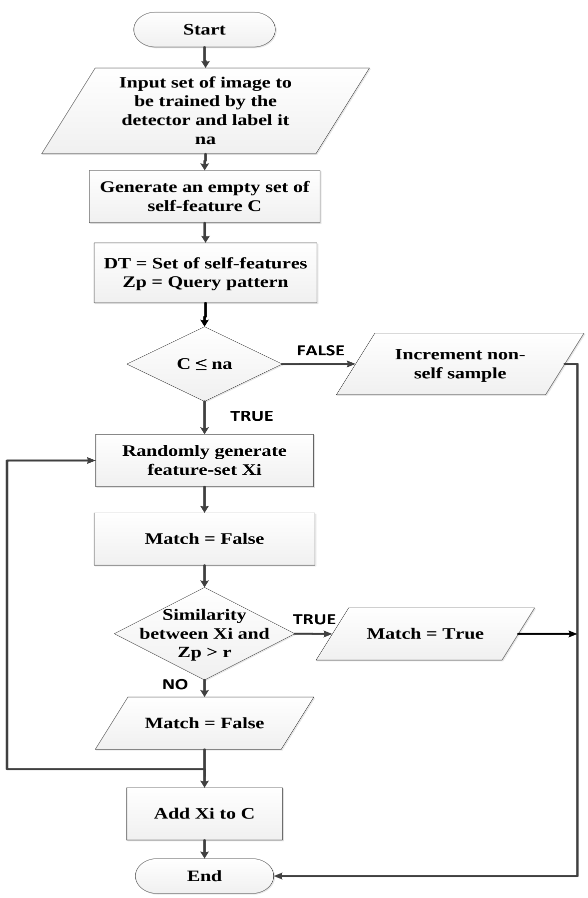

Fig.1. Flowchart of the Implementation of NSA

Algorithm 3: **Algorithm for Negative Selection (NSA)**

Start
Let n_a be the set of images features (detectors) to be trained;
Generate C as an empty set of self-features;
Let D_T represent the set of self-features Z_P (query pattern);
While $C \leq n_a$ **Do**
Randomly generate set of features x_i;
Match = False;
For each set of $z_p \in D_T$ **Do**
If similarity between x_i and z_p is higher than similarity/affinity threshold r **then**;
Matched = True;
break;
end If
end For
If Matched= False; **Then**
xi is added to C;
end if
End.

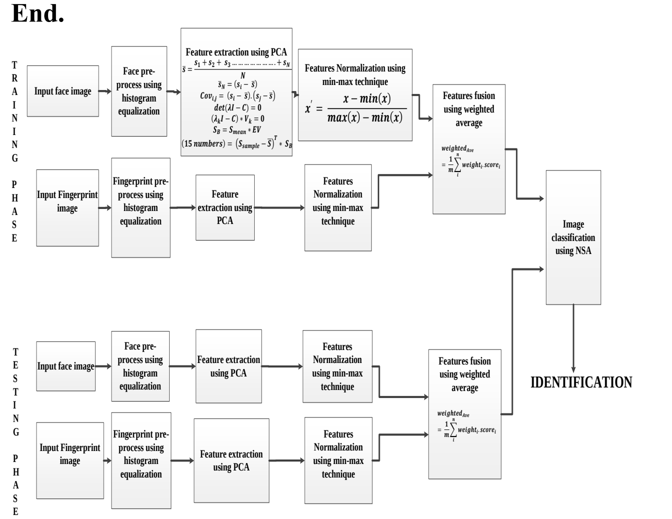

Fig. 2. Block Diagram of the Developed Bi-modal Biometric System of Physiological Traits (face and fingerprint)

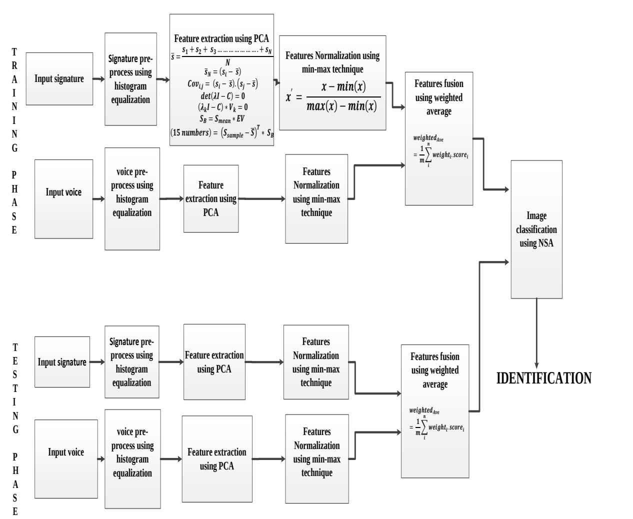

Fig. 3. Block Diagram of the Developed Bi-modal Biometric System of Behavioral Traits (Voice and Signature)

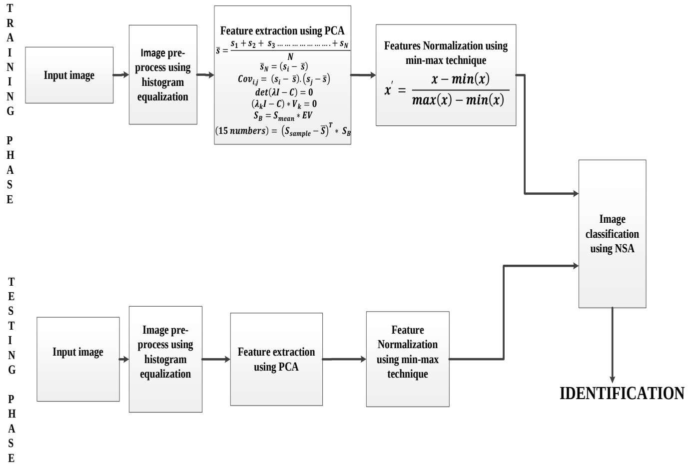

Fig. 4. Block Diagram of a Developed Uni-modal Biometric system

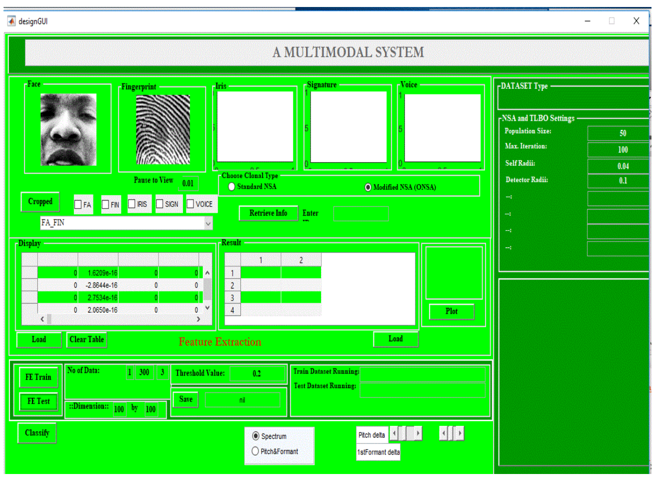

Fig. 5. Graphical user interface for fusion of face and fingerprint

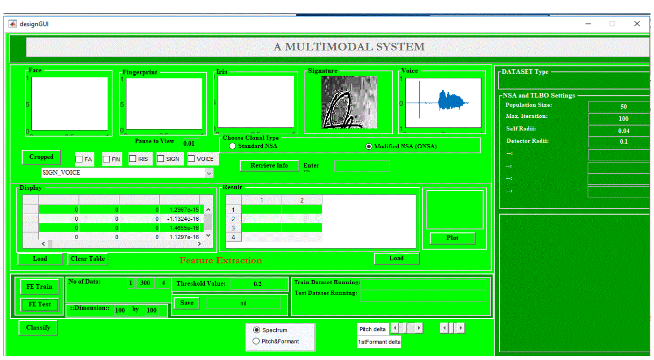

Fig. 6. graphical user interface for fusion of signature and voice

3.2 Data Description

Permission was obtained from individuals whose biometric data were utilized in this study, ensuring a conflict-free relationship between the image owners and the researchers. For the bimodal system incorporating face and fingerprint data, high-resolution images of faces and fingerprints from various perspectives were captured. Facial landmarks and feature points were carefully extracted from facial images, followed by texture mapping of these features. Similarly, minutiae points were extracted from fingerprint images, and ridge pattern information was carefully analyzed. For the bi-modal biometric system combining voice and signature data, high-quality audio recordings and signatures were captured. Salient features were subsequently extracted from the recorded voices and signatures. All collected data met the requisite standards of quality and consistency to facilitate precise identification and verification. Furthermore, robust data storage and security protocols were implemented to safeguard biometric information against unauthorized access or misuse.

IV. Results and Discussions

The implementation of the developed biometric systems was carried out in MATLAB 2016, V 8.1. The performance of the developed bi-modal biometric systems and those of the developed uni-modal biometric systems were compared using TP, TN, FP, FN, FAR, FRR and accuracy. TP and TN describe the rate at which a system correctly accepts and correctly rejects biometric evidence, respectively, while FP and FN describe the rates at which a system incorrectly accepts and incorrectly reject biometric evidence, respectively. The presentation and discussion of the results are as follows.

Table 2 compares the classification accuracies of the bi-modal systems of face and fingerprint (Physiological traits) and Signature and voice (Behavioral traits). It can be seen from the table that, the bi-modal system of behavioral traits produced TP and TN values of 141% and 144%, respectively, while the corresponding values for the physiological traits are 132% and 135%, respectively. Also, bi-modal of behavioral traits generated FN and FP values of 9% and 6%, compared to those of physiological traits that are 18% and 15%, respectively. It can be deduced from the results that fusion of the behavioral traits produced lower false recognition and higher true recognition values compared to those of the fusion of the physiological traits. The lower the false recognition and the higher the true recognition values produced by a system, the more accurate the system, this agrees with [39]. It can also be observed from Table 2 that the behavioral biometric system produced a higher accuracy value of 95% while that of the physiological biometric system is 89%, this also proved that fusion of behavioral traits improves recognition accuracy. Fig. 7 also buttresses the fact established by Table 2 by showing that fusion of behavioral traits has true high recognition values in terms of achieving high TP, TN and accuracy and low false recognition values than fusion physiological traits.

TABLE 2: Result of the classification accuracies of bi-modal systems of physiological and behavioral traits

Metrics	Face and Fingerprint (Physiological traits) %	Signature and Voice (Behavioral traits) %

TP	132	141
FN	18	9
FP	15	6
TN	135	144
FAR	10	4
FRR	12	6
Accuracy	89	95

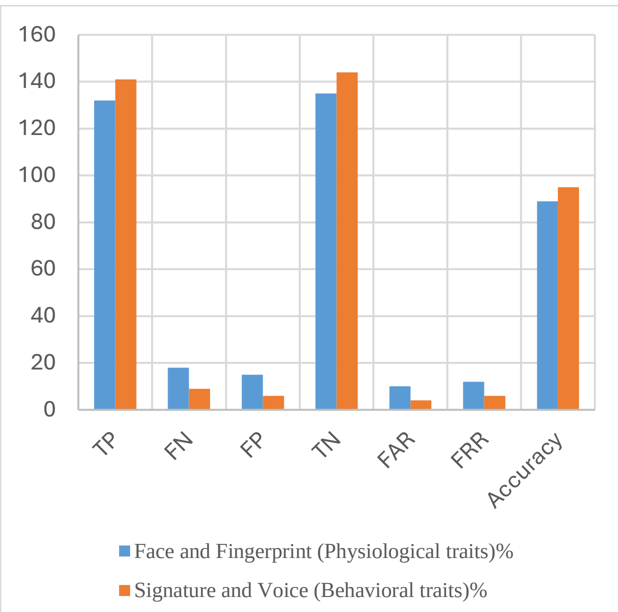

Fig. 7. Comparison of Recognition Accuracy of Fusion of Physiological traits (face and fingerprint) and Fusion of Behavioral traits (signature and voice)

The results of the classification accuracy of the uni-modal biometric systems are presented in Table3. According to the table, the uni-modal biometrics system of voice generated the highest true recognition values and lowest false recognition values by producing TP, TN, FN, and FP of 131%, 134%, 19% and 16%, respectively, followed by the uni-modal system of signature which 130%, 133%, 20% and 17%. While the uni-modal biometric system of face generated the lowest true recognition values and highest false recognition values by producing TP, TN, FN, and FP of 127%, 130%, 23%and 20%, respectively. The uni-modal system of voice also produced the highest accuracy value of 88.33% out of all the uni-modal systems developed. The results from all the uni-modal systems proved that biometric system based on behavioral traits is likely to produce better identification accuracy than biometric system that is based on physiological traits. Fig. 8 supported the fact established by Table 3 by showing that the uni-modal biometric systems of behavioral traits have better recognition accuracy than those of physiological traits. The better performance of behavioral traits can be attributed to the fact that people's sole attention is needed when the behavioral data is collected and human beings can be biased to get perfect identification, this is the other way for physiological traits in which decisions on the nature and quality of data captured almost depends on the capturing devices.

TABLE 3: Result of the classification accuracies of uni-modal systems of face, fingerprint, signature and voice

Metrics	Face (%)	Fingerprint (%)	Signature (%)	Voice (%)
TP	127	128	130	131
FN	23	22	20	19
FP	20	19	17	16
TN	130	131	133	134
FAR	13.33	12.67	11.33	10.67
FRR	15.33	14.67	13.33	12.67
Accuracy	85.67	86.33	87.67	88.33

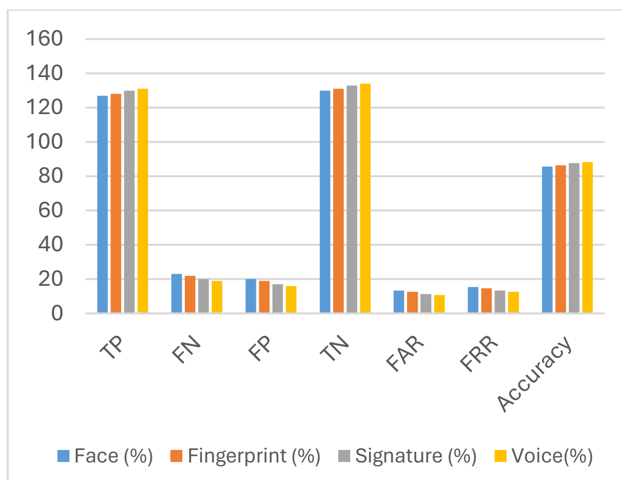

Fig. 8. Comparison of Recognition Accuracy of uni-modal Systems of Face, Fingerprint, Signature, and Voice

V. CONCLUSIONS

This study compares the recognition accuracies of fusion of behavioral traits and fusion of physiological traits in biometric systems. The study was able to establish that bi-modal behavioral traits have better recognition accuracy than that of physiological traits. To further prove the assertion, uni-modal systems of all the biometric traits considered in the work were also developed and it was discovered that the uni-modal systems of behavioral traits outperformed those of physiological traits. However, high recognition of bi-modal system proved that fusion of biometric traits increases the system recognition accuracy. The performances of the developed systems were compared using the following performance evaluation metrics: TP, TN, FN, FP, FAR and FRR and Accuracy.

Conclusively, fusion of biometric traits increases the overall system accuracy.

Future improvement in the work

The following are recommended for future improvement in the developed systems:

• The recognition accuracy of biometric system can be improved by fusing features of both behavioral and physiological traits.

• Data used in this work were collected in an uncontrolled environment (dynamic recognition), implementation of the developed system can also be done using data collected in a control environment (static recognition), to see the effect this will the recognition accuracy.

REFERENCES

[1] D. Dasgupta, K. KrishnaKumar, D. Wong and M. Berry" Negative selection algorithm for aircraft fault detection. In Artificial Immune System" *Third International Conference, ICARIS 2004, Catania, Sicily, Italy*, **1-13**, 2004.

[2] Ji, Zhou, and Dipankar Dasgupta. "Applicability issues of the real-valued negative selection algorithms." *In Proceedings of the 8th annual conference on Genetic and evolutionary computation*, 111-118. 2006.

[3] Chen, Jie, Senyao Chen, Cunbao Ma, Zhengdong Jing, and Qingshan Xu. "Fault detection of aircraft control system based on negative selection algorithm." *International Journal of Aerospace Engineering,* 2020, **1-10**, 2020.

[4] J. de L. Costa, … L. de C.-2019 X. L., and undefined 2019, "Sensitivity analysis of the negative selection algorithm applied to anomalies identification in builds," *ieeexplore.ieee.orgJC de Lima Costa, LN de Castro, C de Paula Bianchini2019 XLV Latin American Computing Conference (CLEI)*, **1-6,** 2019.

[5] S. Hosseini, A. E. Nezhad, and H. Seilani, "Botnet detection using negative selection algorithm, convolution neural network and classification methods," *Evolving Systems,* 13 (1), **101-115,** 2022.

[6] Q. Jin, M. M, "A method to construct self set for IDS based on negative selection algorithm," *ieeexplore.ieee.orgQ Jin, M Ming2011 International Conference on Mechatronic Science, Electric,* **1051-1053**, 2011.

[7] M. Mousavi, A. Bakar, … S. Z.-T. J. "Negative selection algorithm for dengue outbreak detection," *Journals.tubitak.gov.trM Mousavi, AA Bakar, S Zainudin, ZA LONG, M Sahani, M VakilianTurkish Journal of Electrical Engineering and Computer Sciences,* 21(8), **2345–2356**, 2013.

[8] M. Pamukov, V. Poulkov, "Multiple negative selection algorithm: Improving detection error rates in IoT intrusion detection systems," *IEEE international conference on intelligent data acquisition and advanced computing systems: technology and applications (IDAACS),* 1, **543-547**, 2017.

[9] Y. Ren, X. Wang, C. Z.-I. T., "A novel fault diagnosis method based on improved negative selection algorithm," *IEEE Transactions on Instrumentation and Measurement,* 70, **1-8**, (2020).

[10] M. O. Balogun, L. Adeola Odeniyi, E. Olusola Omidiora, S. O. Olabiyisi, and A. S. Falohun, "Optimized Negative Selection Algorithm for Image Classification in Multimodal Biometric System," *Acta Informatica Pragensia*, 12 (1), **3-18**, 2023.

[11] S. A. Dhole, J. K. Patil, S. M. Jagdale, H. G. G. Reddy, and V. D. Gowda, "Multimodal Biometric Identification system using Random Selection of Biometrics," *SSRG International Journal of Electrical and Electronics Engineering*, 10(1), **63-73,** 2023.

[12] A. Booysens and S. Viriri, "Exploration of Ear Biometrics Using EfficientNet," *Comput Intell Neurosci*, 2022, **1-14,** 2022.

[13] S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, "Biometrics recognition using deep learning: a survey," *Artif Intell Rev,* 56(8), **1-49**, 2023.

[14] J. S. Mane and S. Bhosale, "Advancements in biometric authentication systems: A comprehensive survey on internal traits, multimodal systems, and vein pattern biometrics," *Revue d'Intelligence Artificielle*, 37(3), **709-721**, 2023.

[15] S. Ahmad, R. Pal, and A. Ganivada, "Rank level fusion of multimodal biometrics using genetic algorithm," *Multimed Tools Appl*, 81(28), **40931-40958**, 2022.

[16] V. Sandhya and N. P. Hegde, "Patch Based Sclera and Periocular Biometrics Using Deep Learning," *International Journal of Computer Network and Information Security*, 15(2), **15-30**, 2023.

[17] D. Kisku, P. Gupta and K. S. Jamuna, "Multibiometrics Feature level fusion by Graph clustering" *International Journal of Security and Its Applications,* 5(2) **61-74**, 2011.

[18] T. Kovaliuk, N. Kobets, A. Shevchenko, and N. Kunanets, "Multibiometric Identification of Computer Network Users in the Distance Learning Process," 17 *International Scientific and Technical Conference on Computer Sciences and Information Technologies,* **274-278**, 2022.

[19] A. Mondal and S. Roy, "Design and development of fusion-based expert system for multimodal biometric recognition with facemask authentication," *International Journal of System of Systems Engineering*, 13(2), **123-139**, 2023.

[20] P. Szczuko, A. Harasimiuk, and A. Czyżewski, "Evaluation of Decision Fusion Methods for Multimodal Biometrics in the Banking Application," *Sensors,* 22(6), **2-25**, 2022.

[21] K. Chenni and N.-E. Boukezzoula, "Enhancing Person Identification with Score Fusion of Biometric Modalities," *International Conference on Pioneer and Innovative Studies*, 1, **28-33**, 2023.

[22] Z. Akhtar and S. Kale, "Security analysis of multimodal biometric systems against spoof attacks" *First Advances in Computing and Communication, Kochi, India,* 2(1), 604-611, 2011.

[23] R. Vyas, T. Kanumuri, G. Sheoran, and P. Dubey, "Accurate feature extraction for multimodal biometrics combining iris and palmprint," *Journal Ambient Intell Humaniz Comput,* 13(12), **5581-5589**, 2022.

[24] S. Hosseini and H. Seilani, “Anomaly process detection using negative selection algorithm and classification techniques,” *Evolving Systems*, 2(3), **769-778,** 2021.

[25] R. Zhang, X. X.- Complexity, and undefined, “A clone selection based real-valued negative selection algorithm” *Complexity*, 2018, **1-20**, 2018.

[26] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, “ECG and fingerprint bimodal authentication” *Sustainable cities and society 40*, **274-283**, 2018.

[27] K. Okokpujie, J. Abubakar, S. John, E. Noma-Osaghae, C. Ndujiuba, and I. P. Okokpujie, “A secured automated bimodal biometric electronic voting system,” *IAES International Journal of Artificial Intelligence*, 10(1), **1-8**, 2021,

[28] B. A. Joseph “Automated Voting System Using Bimodal Identification and Verification Technique,” *Annals of Computer Science Series*, 15(1), **117-123**, 2017.

[29] J. Xue and H. Zhou, “Physiological-physical feature fusion for automatic voice spoofing detection,” Front Comput Sci, 17(2), **172318**, 2023.

[30] R. Srivastava, D. S.- VLSI, M. and W. Technologies, and undefined 2022, “Human Authentication Using Score Level Fusion of Face and Palm Print Biometrics” Select Proceedings of ICVMWT, **55-64,** 2021.

[31] M. H. Safavipour, M. A. Doostari, and H. Sadjedi, “Deep Hybrid Multimodal Biometric Recognition System Based on Features-Level Deep Fusion of Five Biometric Traits” *Comput Intell Neurosci*, 2023, **1-16**, 2023.

[32] A. Herbadji et al., “Combining multiple biometric traits using asymmetric aggregation operators for improved person recognition” *Symmetry*, 12(3), **2-19**, 2020 .

[33] B. Al-sellami Babasaheb Ambedkar et al., “Overview of Biometric Traits” *Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, **107-113**, 2021.

[34] C. Medjahed, A. Rahmoun, C. Charrier, and F. Mezzoudj, “A deep learning-based multimodal biometric system using score fusion” *IAES International Journal of Artificial Intelligence*, 11(1), **65-80**, 2022.

[35] Y. Jiang, P. Shen, L. Zeng, X. Zhu, D. Jiang, and C. Chen, “Cancelable biometric schemes for Euclidean metric and Cosine metric” *Cybersecurity*, 6(1) , **1-20**, 2023.

[36] N. Alay and H. H. Al-Baity, “Deep learning approach for multimodal biometric recognition system based on fusion of iris, face, and finger vein traits” *Sensors (Switzerland)*, 20(19), **5523**, 2020.

[37] T. R. Yashavanth and M. Suresh, “Performance Analysis of Multimodal Biometric System Using LBP and PCA” *Proceedings: IEEE International Conference on Recent Trends in Electronics and Communication*, **1-5,** 2023.

[38] J. He, W. Chen, T. Li, B. Li, Y. Zhu, and M. Huang, “HD-NSA: A real-valued negative selection algorithm based on hierarchy division” *Appl Soft Comput*, **112**, 2021.

[39] A. Kumar, S. Jain, and M. Kumar, “Face and gait biometrics authentication system based on simplified deep neural networks,” *International Journal of Information Technology (Singapore), vol. 15(2),* ***1005–1014****, 2023.*