[1.] Monsurat O. BALOGUN, [2.] Bilkisu JIMADA–OJUOLAPE, [3.] Latifat A. ODENIYI

IMPROVING HUMAN RECOGNITION IN BIOMETRIC SYSTEMS USING NEGATIVE SELECTION ALGORITHM (NSA)

[1.]Department of Electrical and Computer Engineering, Faculty of Engineering and Technology, Kwara State University Malete, Ilorin, Kwara State, NIGERIA.
[2.]Department of Electrical and Computer Engineering, Faculty of Engineering and Technology, Kwara State University Malete, Ilorin, Kwara State, NIGERIA.
[3.]Department of Mathematics and Computer Science, Koladaisi University Ibadan, Oyo State, NIGERIA

Abstract: The Negative Selection Algorithm (NSA), inspired by the human immune system, has wide–ranging applications including intrusion detection, anomaly detection, and pattern recognition, but its application in human recognition has not been thoroughly explored. This study investigates its potential for human identification, particularly in bi–modal systems that combine physiological and behavioral traits. 2400 sample images from 200 individuals were collected and divided into training, testing, and validation data sets. Images were pre–processing and principal component analysis was used to select salient features. These selected features were fused at the feature level using the weighted average method and NSA was used as classifier. The behavioral feature–based system achieved a remarkable 95% accuracy rate, with true positive (TP) and true negative (TN) rates of 141% and 144%, respectively. In comparison, the physiological traits–based system achieved an 89% accuracy rate. The voice–based uni–modal system outperformed others, with TP and TN rates of 131% and 134%, respectively, with accuracy rate of 88.33%. These findings established the advantages of combining biometric features to enhance system accuracy. It also demonstrates that NSA can significantly improve the precision of biometric systems classification. The developed biometric systems can be emulated in any system that requires ultra–level of security.
Keywords: Behavioral trait, biometric feature, bi–modal biometric, Multi–biometric, Negative Selection Algorithm

1. INTRODUCTION

The Negative Selection Algorithm (NSA) also known as Artificial Immune Systems has emerged as a significant technique within the realm of 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 (Gupta and Dasgupta 2022). By harnessing this biological inspiration, the NSA has proven its potential as a powerful computational tool. It exhibits the capacity to identify and eliminate undesirable entities while preserving and selecting the most suitable ones, this significantly contributed to its effectiveness as an efficient problem–solving approach. The implementation of NSA algorithm in anomalous and fault detection has been considered in several studies NSA was used by Ilhan et al., (2010) to detect faults and anomalies in system. NSA was utilized by Jie et al., (2020) and Dipankar et al., (2004) to find errors in the aviation control system. Jlio et al., (2019) conducted sensitivity analysis of the negative selection algorithm's usage in anomaly detection systems. For Botnet detection, Hosseini et al., (2021) hybridized NSA with other human–inspired algorithms. Jin et al., (2011) constructed a self–set for identity–based fault detection using the NSA. NSA was utilized by Maryam et al., (2013) to detect the possibility of dengue outbreaks. Multiple Negative Selection Algorithm was used by Marin and Vladimir (2017) to reduce detection error rates in IoT intrusion detection systems. A brand–new fault diagnosis technique was created by Yanheng et al., in 2020 using an upgraded negative selection algorithm. 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 the identity of a person based on their biological and behavioral characteristics. It has been established that the best method of 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 (Wendehorst et al., 2022). Biometric identifiers are unique and reliable features of a person's body and behavior that can be measured and compared with an existing database. Biometric identification systems are widely used in security, law enforcement, banking, immigration and so on.

2. BIOMETRIC SYSTEM

Biometric is the process of using the inherent properties of human beings in identity creation (Vivian, 2017). The inherent properties can be physiological (face, fingerprint, iris, palm vain) or behavioral (signature, voice, gait). One of the valuable tools that is used in decision making is identity, which if not well established can leads to so many misinformation (Khanet al., 2011). Identity is a quality that establishes who or what a person or item is. There are two main methods of establishing identity: the conventional/traditional method and the biometric method. The conventional way involves using the information possessed by a person

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

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 (Hong and Jain, 1998). The formal has been proved to be prone to so 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 to be the most reliable and suitable means of human identification (Zahid, 2012). A biometric system uses pattern recognition to identify people by establishing the authenticity of everyone's possession of a certain behavioral or physiological feature (Kisku et al., 2011). 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.

There are different types of multi–biometric systems such as multi–instance, multiple–algorithms, multi–sample, multi–sensor, multi–modal and hybrid biometric system (Shilpa, 2013). 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. A hybrid biometric system incorporates two or more of the many multi–biometric system varieties.

A bi–modal biometric system combines two biometric traits to overcome the probable limitations of uni–modal biometric system (Feng et al., 2004). 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 (Mayhew, 2012). Hence, this work designed bi–modal biometric systems that combined physiological traits (face and fingerprint) and behavioral traits (signature and voice). The six fundamental stages of a bi–modal biometric system are image capture, image preprocessing, feature extraction, feature fusion, classification, and decision–making.

Image capturing is a stage of a biometric system at which the required raw biometric evidence or traits are acquired. This stage is very important because it has a great influence on the overall system performance. Image pre–process involves error removal and fine–tuning of the acquired image (Sumathi and Marlin, 2013). 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. Feature normalization brings all the feature into common domain and helps in preventing a feature from dominating the feature samples. 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 (Prabhakar et al., 2003). 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.

3. LITERATURE REVIEW

Numerous studies have been conducted on how to enhance the functionality of biometric identification systems, particularly multi–biometric systems. The best level of fusion and the appropriate fusion technique have always been contentious issues in multi–biometric systems. In a multi–biometric system, features fusion can be done at various levels, including the sensor level, feature level, match score, and abstract/decision level fusion. The level of precision required from the system, the type of biometric qualities that are taken into consideration, the volume of data, and the fusion technique utilized in a certain system are some of the aspects that influence the optimal fusion level to choose. Numerous researchers have used various fusion approaches at various levels of fusion to enhance the performance of multi–biometric systems, as discussed below.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

In their 2021 study, Hosseini and Seilani employed Negative Selection for detecting anomalies within a system, where anomalies were defined as elements not conforming to the system's norm. The authors introduced an innovative approach for anomaly process detection, merging Negative Selection with a classification algorithm. They conducted experiments using the CICIDS 2017 and NSL–KDD datasets, each with distinct feature sets but an equal number of detectors. To refine the dataset, they utilized the WEKA tool for correlation–based feature selection. The effectiveness of their technique was assessed using various machine learning algorithms, including logistic regression, random forest, decision tree, and K–nearest neighbors. Notably, the results revealed that their approach, referred to as NSA, outperformed all other algorithms in the context of anomaly detection.

Johnson and Davis (2019) introduce a groundbreaking approach that integrates the negative selection algorithm with a clonal selection mechanism. The primary objective of their proposed technique is to enhance the algorithm's proficiency in distinguishing between patterns that are part of the system's norm (self) and those that deviate from it (non–self). By subjecting their method to thorough assessments using well–established benchmark datasets and conducting comprehensive comparisons with other pattern recognition methods, the study demonstrates its ability to deliver competitive performance. Furthermore, it underscores the algorithm's promising potential in tackling intricate challenges within the realm of pattern recognition.

Anderson and Wilson (2018) propose a method that utilizes the Negative Selection Algorithm (NSA) to detect abnormal behavior in control systems. By generating a set of detectors that capture normal system behavior, the algorithm effectively identifies deviations as potential anomalies. Real–world experiments conducted on industrial control systems validate the approach's effectiveness in detecting anomalies, thereby enhancing system security and reliability.

Thompson and Brown (2020) introduce a method that leverages the negative selection algorithm to detect faults and disturbances in power system measurements. The algorithm undergoes training using data from normal operating conditions, and any deviations from this baseline are identified as potential faults. By conducting assessments on a real–world power system dataset, the research illustrates the algorithm's proficiency in accurately detecting a wide range of fault types. This highlights NSA promising role in enhancing the reliability of power systems.

In (Gawande and Hajari, 2013) a multi–biometric system that integrated facial and palm–print traits at the feature level was developed. This fusion of the features was achieved through the utilization of an enhanced K–medoids clustering algorithm in conjunction with an isomorphic graph. The process involved partitioning the set of invariant features into K clusters, employing the Perturbing Around Method (PAM). To determine the most suitable pair of graphs, an iterative relaxation algorithm was applied to all possible isomorphic graphs, specifically for pairs of correlated facial and palm–print images. The experimental outcomes demonstrated a notable enhancement in system performance attributed to the K–medoids partitioning algorithm, resulting in an impressive achievement of a 0.0% False Acceptance Rate (FAR) and an impressive 99.5% recognition rate.

Balogun et al., (2023) devised a comprehensive multi–biometric system that amalgamated features from various sources, including face, fingerprint, iris, signature, and voice. They amassed a substantial dataset comprising over 6000 biometric samples from individuals of African descent. In this research, two distinct biometric systems were developed: one dedicated to each individual trait (uni–modal), and the other that ingeniously combined all these traits into a multi–modal system. The process entailed feature extraction through Principal Component Analysis (PCA), and for the multi–modal system, these extracted features were integrated at the feature level using the Weighted Average Method (WAM). Additionally, they employed the Optimized Negative Selection Algorithm as classifiers. In the comparative analysis of these biometric systems, it was revealed that the multi–modal system achieved the highest recognition accuracy, boasting an impressive 98.33% recognition rate at a recognition threshold of 0.98. In contrast, the uni–modal systems yielded recognition rates of 90.33%, 89.67%, 89.00%, 88.33%, and 87.67%, respectively, at the same recognition threshold.

In (Nulu et al., 2014) a comprehensive biometric system was developed, incorporating three distinct biometric characteristics: facial features, palm print patterns, and gait signatures. The selection of relevant features was achieved through the application of the Geometry Preserving Projections (GPP) algorithm. GPP was chosen for its ability to effectively discriminate between different classes while still retaining the subtle variations within similar classes. The training process for each biometric trait involved sub–space

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

learning using the GPP algorithm, followed by classification in a reduced–dimensional space. To facilitate this research, two specific data arrays were constructed, known as YALE–HKPU–USF and FERET–HKPU–USF. The results of this study indicated a recognition rate of 90.22% for the YALE–HKPU–USF dataset and an impressive 93.67% for the FERET–HKPU–USF dataset when employing the Kernel Geometry Preserving Projections (KGPP) method.

Falohun et al., (2016) fused the features of face and palm print at feature level using PCA and ICA for features extraction 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.

In Viriri and Tapamo (2012) an innovative multi–modal biometric system was introduced, merging the distinctive characteristics of iris and signature biometrics. To combine these features effectively, a user–score–based weighing technique was employed, assigning specific weights that represented the contribution of each biometric attribute to the final score output. Remarkably, this system exhibited remarkable performance results, boasting a remarkably low False Rejection Rate (FRR) of only 0.08% and an equally impressive False Acceptance Rate (FAR) of just 0.01%.

Kounoudes et al., (2008) developed a system that combines the unique traits of hand geometry and palm–print features. The feature extraction process involved Discrete Wavelet Transform, and classification was carried out using the Support Vector Machine (SVM) algorithm. Feature fusion was applied at the match score level. The experimental results were quite impressive, achieving a Genuine Acceptance Rate (GAR) of 99.47% and a False Acceptance Rate (FAR) of 0% when evaluated with an existing GPDS database. However, the limitation of this work was identified. Specifically, if a large dataset were used to test the developed system, there might be a potential reduction in accuracy.

Zhang et al., (2008) developed a multimodal biometric system by integrating voice, face, finger, and palm features collected from a group of 30 individuals, utilizing the BOLYBIO datasets. Data collection involved five instances for each biometric trait (multi–instance), with four instances used for training and one for testing. To consolidate the information from the individual traits, a single voting scheme was applied at the output level. In this approach, a user is identified if many of the modalities confirm their identity; otherwise, the identity is rejected. This strategy capitalizes on the concept that weaker classifiers can complement stronger ones, resulting in enhanced performance in terms of both False Acceptance Rate (FAR) and False Rejection Rate (FRR), while preserving the excellent performance of the single modality system. The evaluation of the results demonstrated that the multi–modal system, employing the voting scheme at the output level, achieved the most favorable results with a remarkably low False Acceptance Rate of 1.23% and an equally impressive False Rejection Rate of 0.8%.

Khan et al., (2011) developed a system that combines a selected set of facial images with the closest matching finger vein patterns at the score level fusion. This integration process relies on minimizing the Euclidean distance between these features. Face images were captured using a low–resolution web camera, while finger vein images were obtained using a HITACHI finger veins device. The dataset consisted of data from 35 CAIRO staff and students, and the system was simulated in a C# environment. Both facial and finger vein data underwent extraction using Linear Discriminant Analysis (LDA). The evaluation of the results revealed remarkable performance, with an impressively low False Acceptance Rate (FAR) of 0.000026 and a high Genuine Acceptance Rate (GAR) of 97.4%. It's important to note that the system was tested on a relatively small database, which contributed to the high GAR value obtained.

Wendehorst et al., (2022) developed a multi–biometric system by combining the features of iris, fingerprint, face, and palm–print. Fingerprint samples were gathered from a college, irises were sourced from the CASIA database, and facial and palm geometry data were obtained from standard databases. The fusion of features occurred at the feature level using the convolution theorem. The resulting feature vectors were multiplied together to create the final multi–modal template. For classification, probabilistic neural network (PNN) and radial basis function (RBF) methods were employed. The comparison of query features with the existing database for identification purposes was facilitated by an Adaptive Cascade approach, which utilized mean and variance values. In the verification phase, a back–propagation neural network (BPNN) was utilized to classify query data as either genuine or imposter. The experiment yielded the following results: a 2% False Acceptance Rate (FAR), a 1.2% False Rejection Rate (FRR), and a Genuine Acceptance

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

Rate (GAR) of 98.8%. However, it's important to note that these impressive performance metrics were obtained from a heterogeneous dataset, leading to some skepticism regarding the feasibility of such high performance in real–world scenarios.

Therefore, in this study, two bi–modal biometric systems: one combining facial and fingerprint data (physiological traits), and the other merging signature and voice data (behavioral traits) are developed. To assess the effectiveness of these two systems, their recognition accuracy was evaluated by comparing metrics such as True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN), False Acceptance Rate (FAR), False Rejection Rate (FRR), and overall Accuracy with those of the individual biometric systems of face, fingerprint, signature, and voice.

4. METHODOLOGY

In this research, six different biometric systems were developed. These included a bi–modal biometric system that combined facial and fingerprint data (physiological traits), another bi–modal system merging signature and voice data (behavioral traits), and individual uni–modal systems for each of the biometric traits. The developed biometric systems were employed for the purpose of identification and their performances were compared using various metrics, such as True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN), False Acceptance Rate (FAR), False Rejection Rate (FRR), and overall Accuracy.

A total number of 2400 of biometric samples were captured using appropriate devices. Facial data was obtained using a CMITECH face and iris camera, fingerprints were captured using a digital personnel fingerprint capturing device, signatures were recorded using a Topaz T device, and voices were recorded using an Android phone's voice recorder. The devices were positioned in proximity for user convenience.

To prepare the images for analysis, they were the first image pre–processed. Image pre–processing involved several steps: including error elimination, pattern localization, and identification of significant image features. Face, fingerprint, and signature images were converted to grayscale and histogram equalization, image cropping, and binarization were also performed on the images. Voice data underwent pre–processing such as analog–to–digital conversion, silence detection, pre–emphasis, and windowing.

Follows by image pre–processing are features extraction using Principal Component Analysis (PCA). PCA was chosen because of its capability to extract optimal/salient features from digital representation without compromising the image quality. Selected physiological traits (face and fingerprint) were fused at the feature level using weighted average method. Behavioral features (signature and voice) were also combined at the feature level using the same fusion method. However, due to the distinctive nature of the biometric traits involved, the selected features were normalized before fusion using the min–max normalization technique. Algorithm 1 outlines the steps of the min–max normalization process, and the formula representation of the algorithm is shown in Equation 9.

PCA Steps for Feature Extraction

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

Given N–samples of any of the considered traits, such as fingerprint images, the mean vector was computed as follows:

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

For each image vector, the mean–adjusted vector was calculated as follows:

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

All the mean–adjusted vectors were combined to create the mean–adjusted matrix:

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

Therefore, covariance of a matrix with dimensions 150*150, which is equivalent to an (i x j) matrix is:

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

where,

$\bar{s}$ is the calculated mean vector
s_i is the i^{th} image vector
s_j is the j^{th} image vector

The eigenvalues of the covariance matrix were computed using Equation (5).

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

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

where,

det is the determinant of the matrix
λ is the Eigen values associated with the matrix
I is the identity matrix

The corresponding eigenvector for a given high eigenvalue is determined by employing Equation (6):

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

where,

λ_k= One of the highest Eigen values kept
C = covariance matrix
V_k= Eigen vector

As a result, the first 15 high eigenvalues are selected, leading to the existence of 15 corresponding eigenvectors denoted a (V_1,……..,V_{15}).

Eigen Vector (EV)= $V_1, \ldots\ldots\ldots\ldots\ldots\ldots, V_{15}$

Basic vector S_B is determined using Equation (7):

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

where, S_{mean} is the mean adjusted matrix with dimension.
EV is the Eigen vector matrix

Each sample is subsequently represented as a linear combination of fundamental vectors using Equation (8):

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

where,

S_{sample}= The sample to be represented using basic vector
$\overline{S}$ = The mean adjusted vector with dimension $(15 * 1)$
S_B = The basic vector with dimension $(150 * 150)$

Through these procedures, each image that was originally represented by 22,500 number is now expressed as a concise set of 15 numbers.

Algorithm 1: Min–max normalization

Start

Create a vector x that contains selected feature 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 empty set of x'.

For each $x_i, \in x$,
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 initial 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 applied to unify all the chosen features into a consistent domain, thereby facilitating their straightforward fusion. Feature fusion was accomplished using the Weighted Average Method described in Equation (10). This process entailed combining all the features derived from the biometric traits. The step–by–step execution of Equation 2 is outlined in Algorithm 2.

Algorithm 2: Weighted Average

Start

Initialize variables:

$sum_scores = 0$
$sum_weights = 0$

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

$\text{weighted_ave} = 0$
IF $\text{core} = \text{weight}$.
For (i=1; i= n; ++i)
$\text{Sum_score} = \sum_{i=1}^{n} \text{score}_i$
$\text{sum_weight} = \sum_{i=1}^{n} \text{weight}_i$
` $\text{weighted_score} = \text{sum_score} * \text{sum_weight}$
End For
End IF

$$\text{weighted}_{\text{ave}} = \frac{1}{m}\sum_{i=1}^{n} \text{weighted_score}$$

Return $\text{weighted}_{\text{ave}}$
End.

$$\text{weighted}_{\text{Ave}} = \frac{1}{m}\sum_{i}^{n} \text{weight}_i.\text{score}_i \quad (10)$$

where m represents the value employed to normalize the score within the range of 0 to 1, n denotes the total number of modalities, $weight_i$ signifies the weight associated with each individual modality and $score_i$ corresponds to the matching score for each single modality.

The classification process was carried out using the Negative Selection Algorithm (NSA). The selection of NSA as the classifier in this study is attributed to its capability to provide solutions to computational challenges, including computer security, network security, and anomaly detection problems, among others (Forrest et al., 1994). NSA emulates the operational principles of the mammalian immune system, with its primary objective being the classification of binary data or bit strings, referred to as features, into "self" (normal) or "non–self" (anomalous). The fundamental concept involves generating a set of detector features that can be utilized to classify new data or patterns (unseen data) as either "self" or "non–self." According to (Hosseini et al.,2021), NSA encompasses two distinct phases: the learning phase and the 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 (Ren et al., 2021). To examine the performance of biometric system, the system reactions to large number of queries features from both authorized and non–authorized subjects is 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 as a result 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 Figure1 illustrates flowchart of the NSA implementation. Shown in Figures 2, 3 and 4 are the block diagrams of the developed biometric systems, while Figure 5 and 6 showed the graphical user interface for the two developed bi–modal biometric systems implemented in MATLAB.

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;

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

Match = False;
For each set of $z_p \in D_f$ **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

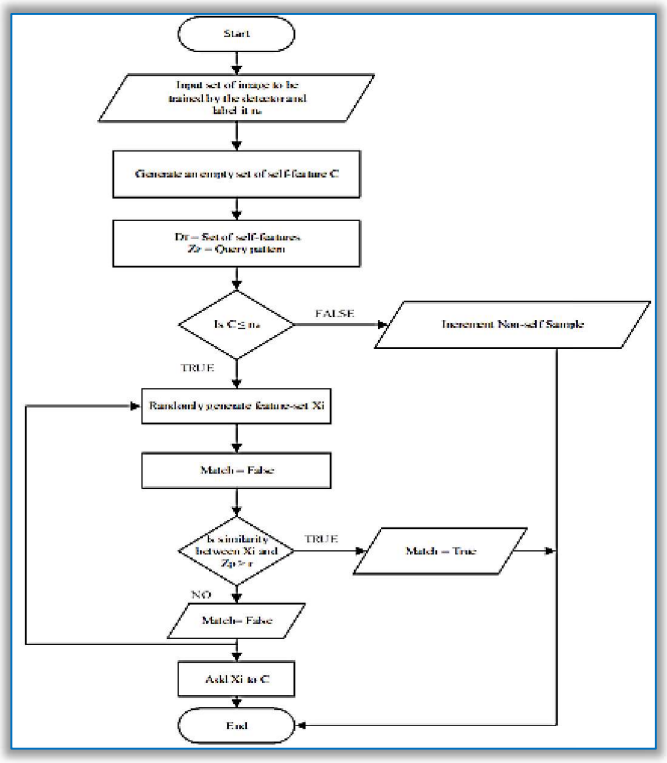


Figure 1: Flowchart of the implementation of NSA

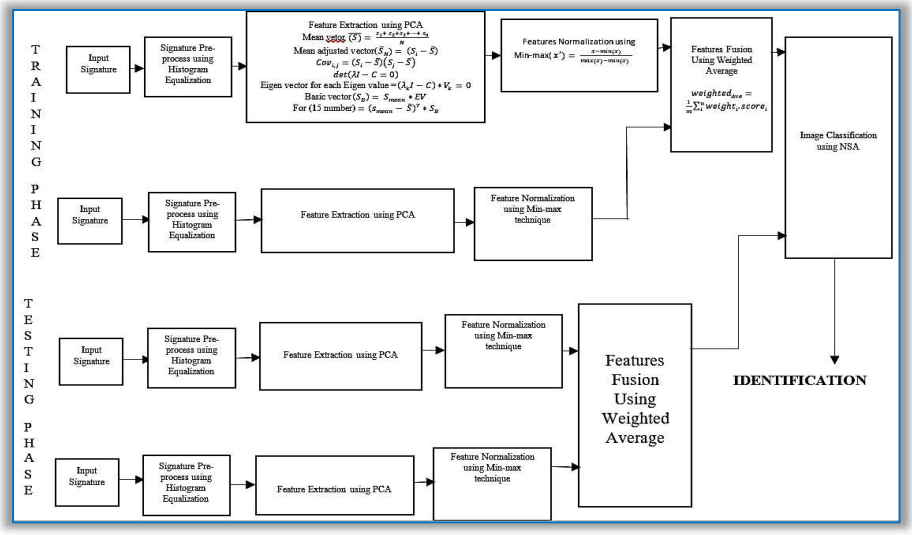


Figure 2: Block Diagram of the Developed Bi–modal Biometric System of Physiological Traits (face and fingerprint)

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

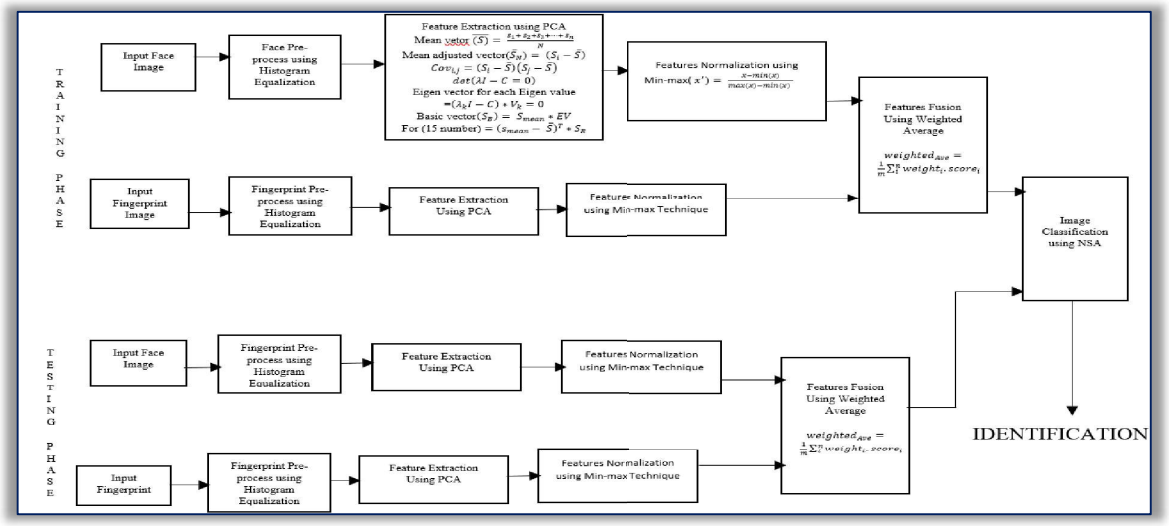


Figure 3: Block Diagram of the Developed Bi–modal Biometric System of Behavioral Traits (face and fingerprint)

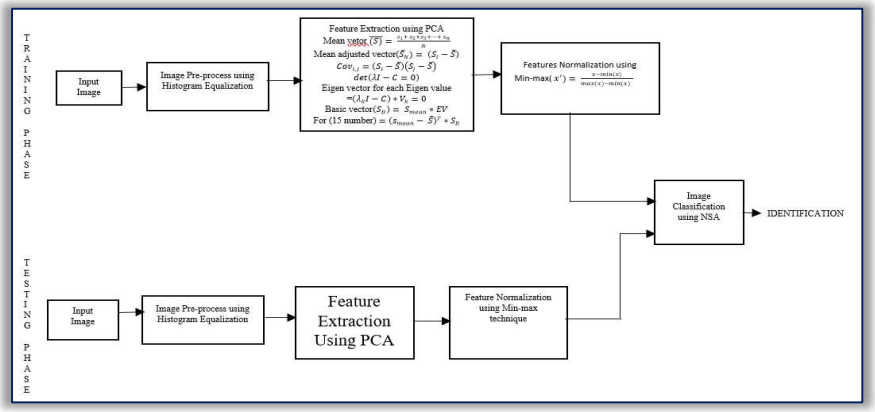


Figure 4: Block Diagram of the Developed Uni–modal Biometric Systems

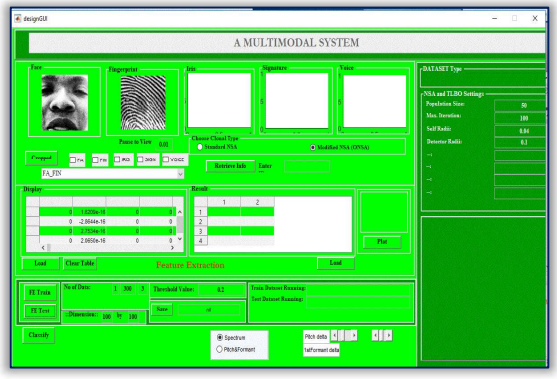


Figure 5: Graphical user interface for fusion of face and fingerprint

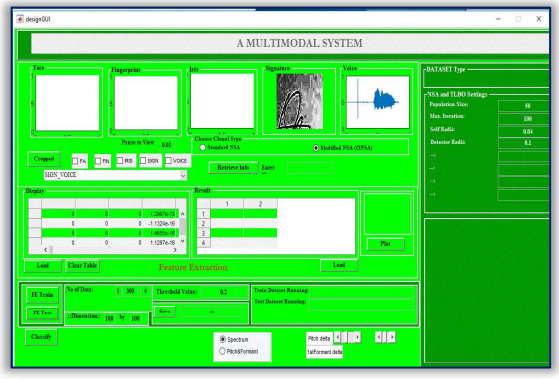


Figure 6: graphical user interface for fusion of signature and voice

5.DISCUSSION OF RESULT

The implementation of the designed biometric systems was executed using MATLAB 2016, Version 8.1. To evaluate and compare the performance of the developed bi–modal biometric systems with that of the developed uni–modal biometric systems, various metrics were employed. These metrics include True Positives (TP), True Negatives (TN), False Positives (FP), False Negatives (FN), False Acceptance Rate (FAR), False Rejection Rate (FRR), and accuracy.TP and TN signify the rates at which a system accurately accepts and accurately rejects biometric evidence, respectively. Conversely, FP and FN represent the rates at which a system incorrectly accepts and incorrectly rejects biometric evidence. The results are presented and discussed in the following sections.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

Table 1: 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

It can be seen from Table 1 that the bi–modal system that combines signature and voice (behavioral traits) yielded TP and TN values of 141% and 144%, respectively, while the corresponding figures for the combination of face and fingerprint (physiological traits) were 132% and 135%, respectively. Furthermore, the bi–modal system incorporating behavioral traits resulted in FN and FP values of 9% and 6%, in contrast to physiological traits exhibited 18% and 15%, respectively. These results suggest that the fusion of behavioral traits leads to reduced false recognition and increased true recognition rates compared to the fusion of physiological traits. As a general principle, a system with lower false recognition and higher true recognition rates is deemed more accurate, as also affirmed by (Balogun et al., 2023).

Table 1 also illustrates that the behavioral biometric system achieved a higher accuracy rate of 95%, whereas the physiological biometric system achieved 89%. This reaffirms the notion that combining behavioral traits enhances recognition accuracy. Figure 6 further corroborates the findings presented in Table 1, demonstrating that the fusion of behavioral traits exhibits significantly higher true recognition values and lower false recognition values compared to the fusion of physiological traits.

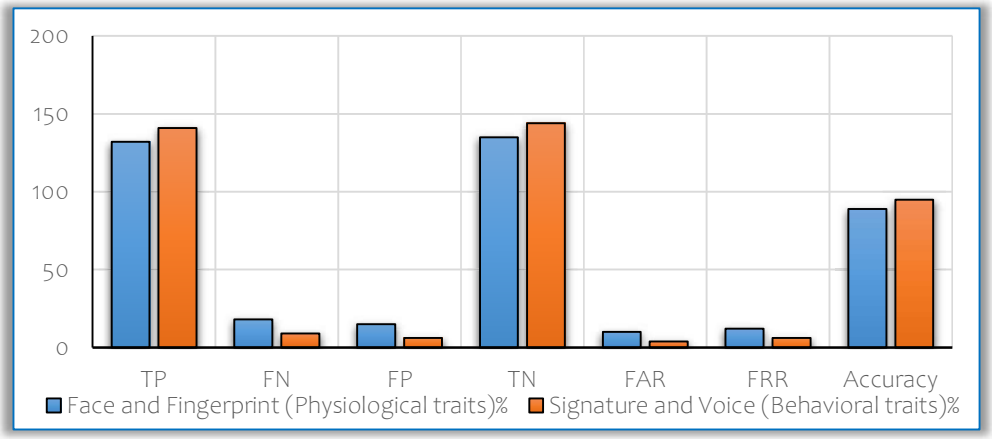


Figure 6: Comparison of Recognition Accuracy of Fusion of Physiological traits (face and fingerprint) and Fusion of Behavioral traits (signature and voice)

Table 2: 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

The results of the classification accuracy of the uni–modal biometric systems are presented in Table2. 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. Figure 7 reinforces the observation established in Table 2, demonstrating that the uni–modal biometric systems

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

based on behavioral traits exhibit superior recognition accuracy compared to those based on physiological traits. The better performance of behavioral traits can be attributed to the fact that people sole attention is needed when the behavioral data is being collected and human being can be bias to get perfect identification, this is the other way for physiological traits in which decision on the nature and quality of data captured is almost depends on the capturing devices.

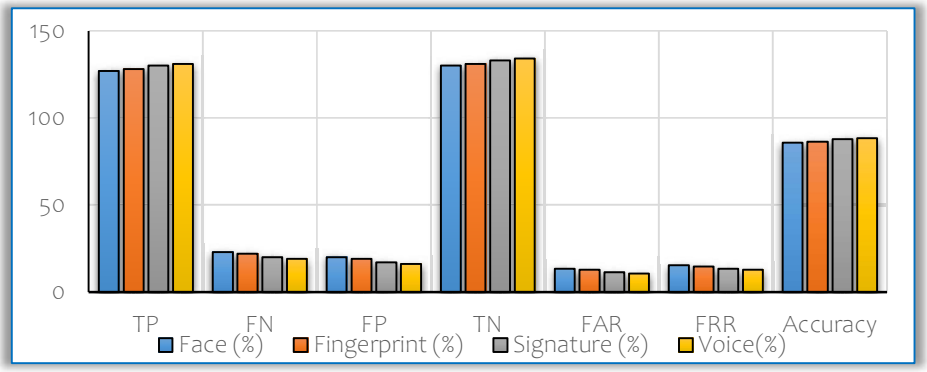


Figure 7: Comparison of Recognition Accuracy of uni–modal systems of face, fingerprint, signature and voice

6. CONCLUSION & FUTURE IMPROVEMENT IN THE WORK

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 has better recognition accuracy than that of physiological traits. To prove further 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 performance of the developed systems was assessed by comparing them using the following performance evaluation metrics: True Positives (TP), True Negatives (TN), False Negatives (FN), False Positives (FP), False Acceptance Rate (FAR), False Rejection Rate (FRR), and Accuracy.

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

Here are some suggested areas for future enhancements to the developed systems:

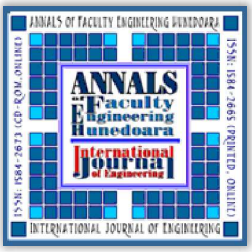
- The identification accuracy of biometric system can be improved by fusing features of both behavioral and physiological traits in a single system.
- Data used in this work were collected in an uncontrolled environment (dynamic recognition), implementation of the developed system can also be done using data collected in a control environment (static recognition), to see the effect this will have on the recognition accuracy.

References

[1] Anderson, M., Wilson, S. (2018). "Negative Selection Algorithm for Anomaly Detection in Industrial Control Systems." IEEE Transactions on Industrial Informatics
[2] Balogun Monsurat Omolara, Odeniyi Latifat Adeola, Omidiora Elijah Olusola, Olabiyisi Stephen Olatunde, Falohun Adeleye Samuel (2023) "Optimized Negative Selection Algorithm for Image Classification in Multimodal Biometric System" Acta Informatica Pragensia, Volume 12, Issue 1.
[3] Dipankar Dasgupta, Kalmanje KrishnaKumar, D Wong, and Misty Berry. Negative selection algorithm for aircraft fault detection. In International Conference on Artificial Immune Systems, pages 1–13. Springer, 2004.
[4] Falohun A. S., Fenwa O. D. and Ajala F. A. (2016). A Fingerprint–based Age and Gender Detection System Using Fingerprint Pattern Analysis; International Journal of Computer Application, 136(4):43–48.
[5] Feng, G. Dong K. Hu D. and Zhang D. (2004). When Faces Are Combined with Palm–prints: A Novel Biometric Fusion Strategy; Biometric Authentication vol. 307.
[6] Forrest S. Perelson A. S., Lawrence A. and Rajes C. (1994). Self–Nonself in Computer, IEEE Proceeding Computer Society Symposium, pp.202–212.
[7] Gawande U., and Hajari K. (2013). Adaptive Cascade Classifier Based Multimodal Biometric Recognition and Identification System; International Journal of Applied Information Systems (IJAIS), 6(2).
[8] Gupta K. D. and Dasgupta D. "Negative Selection Algorithm Research and Applications in the Last Decade: A Review," in IEEE Transactions on Artificial Intelligence, vol. 3, no. 2, pp. 110–128, April 2022
[9] Hong L. and Jain A. (1998). Integrating Faces and Fingerprints for Personal Identification; IEEE. Pattern Anal., 20(12): 1295–1307.
[10] Hosseini S., Nezhad A. E. and Seilani H. (2021). "Botnet detection using negative selection algorithm, convolution neural network and classification methods," Evolving Systems, pp. 1–15.
[11] Hosseini, S., Seilani, H. Anomaly process detection using negative selection algorithm and classification techniques. Evolving Systems 12, 769–778 (2021)
[12] Ilhan Aydin, Mehmet Karakose, and Erhan Akin. Chaotic–based hybrid negative selection algorithm and its applications in fault and anomaly detection. Expert Systems with Applications, 37(7):5285–5294, 2010.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

[13] Jie Chen, 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, 2020.
[14] Jin Q. and Ming M. (2011), "A method to construct self–set for ids based on negative selection algorithm," in 2011 International Conference on Mechatronic Science, Electric Engineering and Computer (MEC). IEEE, 2011, pp. 1051–1053.
[15] Johnson, D., Davis, E. (2019). "Artificial Immune System–Based Negative Selection Algorithm for Pattern Recognition." Pattern Recognition.
[16] Khan M. K., Alghathbar K, and Yusof R. (2011). Multimodal Biometric Recognition Based on Fusion of Low–Resolution Face and Finger Veins; International Journal of Innovative Computing, Information and control, **7**(8): 4679–4689.
[17] Kisku R. D., Gupta P. and Sing J. K. (2011). Multi–biometrics Feature Level Fusion by Graph Clustering; International Journal of Security and Its Applications, **5** (2): 61–74.
[18] Kounoudes A., Tsapatsoulis N., Theodosiou Z. and Milis M. (2008). Multimodal Biometric Data Acquisition Platform and Security System; Biometrics and identity management, Springer, Berlin, Heidelberg, 216–227.
[19] Marin E Pamukov and Vladimir K Poulkov. Multiple negative selection algorithm: Improving detection error rates in iot intrusion detection systems. In 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), volume 1, pages 543–547. IEEE, 2017.
[20] Maryam Mousavi, Azuraliza Abu Bakar, Suhaila Zainudin, Zalizah Awang Long, Mazrura Sahani, and Mohammadmahdi Vakilian. Negative selection algorithm for dengue outbreak detection. Turkish Journal of Electrical Engineering & Computer Sciences, 21(Sup. 2):2345–2356, 2013.
[21] Mayhew S. (2012). UNHCR Introduces New Biometric ID Card for Refugees/ Biometric Update: Biometric Update.com.june 21, 2016, htttp:/www.biometricupdate.com/201606/unhcr–introduces–new biometric–id–card–for–refegee.
[22] Nulu S., Khan R. A., and Rajrhree P. (2014). Equal Error Rate and Audio Digitization and Sampling for Speaker Recognition System; Journal of Computational and Theoretical Nanoscience, 20(5–6):1085–1088.
[23] Prabhakar S., Pankanti S.A. and Jain K. (2003). Biometric Recognition: Security and Privacy Concerns, IEEE Security and Privacy, March 2003, PP. 33–42.
[24] Ren Y., Wang X. and Zhang C. (2021), "A Novel Fault Diagnosis Method Based on Improved Negative Selection Algorithm," in IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1–8
[25] Shilpa Shrivastava (2013). Biometric: Types and its Applications: International Journal of Science and Research (IJSR), 6(14): 204–207.
[26] Sumathi S. and R. Malin (2013). Multimodal biometrics for person authentication using hand images; International Journal of Computer Applications (IJCA), 70(24): 234–240.
[27] Thompson, R., Brown, J. (2020). "Negative Selection Algorithm for Fault Diagnosis in Power Systems." Electric Power Systems Research.
[28] Viriri S. and Tapamo R. (2012). Integrating Iris and Signature Traits for Personal Authentication using User–Specific Weighting; Sensor, 12(4): 4324–4338.
[29] Vivian L.V. (2017). Identity: Personal and Social; Oxford Handbook of Personality and Social Psychology. 2nd Edition: 1–21.
[30] Wendehorst, Christiane and Duller, Yannic, Biometric Recognition and Behavioral Detection (2021). Wendehorst/Duller, Biometric Recognition and Behavioral Detection: Study commissioned by the European Parliament (2021)
[31] Zahid Akhtar (2012). Security of Multimodal Biometric Systems against Spoof Attacks; Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy.
[32] Zhang T., Li X., Tao D. and Yang J. (2008), Multimodal Biometrics Using Geometry Preserving Projections; Pattern Recognition 41(3): 805–813.





ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN–L 1584 – 2665
copyright © University POLITEHNICA Timisoara, Faculty of Engineering Hunedoara,
5, Revolutiei, 331128, Hunedoara, ROMANIA
http://annals.fih.upt.ro