

Fuzzy Logic Approach to Determine Security Level of Biometrics Traits

O.C. Abikoye, K.S. Adewole & N.K. Salahdeen

Department of Computer Science

University of Ilorin

Ilorin, Nigeria

kemi_adeoye@yahoo.com, adewole.ks@unilorin.edu.ng, nsalahdeen@gmail.com

ABSTRACT

One of the methods that use uniquely identifiable physical or behavioral characteristics to identify individuals is Biometrics. As Biometrics becomes the most promising authentication technology, the world is faced with the challenge of choosing the best among the biometrics traits for their security purposes. In this paper, a model is proposed using fuzzy logic approach to evaluate the Biometrics traits in order to determine their security level. Biometrics characteristics categorized by previous researchers in the field of Biometrics was used as knowledge base. The model developed was simulated using Qtfuzzylite 4.0 (A Fuzzy Logic Control Library in C++) and the results show that Fingerprint, Hand Geometry, Hand Veins, Iris, Ear Canal and Palm print have medium security level among the fifteen (15) Biometrics traits considered based on the following metrics; Universality, Uniqueness, Permanence, Collectability, Performance and Circumvention. The results of this simulation further revealed that fuzzy logic approach provides a simple way of drawing definite conclusions from vague and imprecise information.

Keywords: Biometrics traits, Fuzzy logic, Model, Simulation, Security level

African Journal of Computing & ICT Reference Format:

O.C. Abikoye, K.S. Adewole & N.K. Salahdeen (2014). Fuzzy Logic Approach to Determine Security Level of Biometrics Traits. Afr J. of Comp & ICTs. Vol 7, No. 4. Pp 117-130

1. INTRODUCTION

Due to the vulnerability associated with both token-based (e.g. id card) and knowledge-based (e.g. personal identification number) authentication approach has paved way for biometric authentication as the most promising authentication technology whereby certain services have to be restricted to only authorized personal [1]. Biometrics refers to the identification of humans by their characteristics or traits [2]. Characteristic is a special quality or trait that makes a person, thing, or group different from others. Biometric characteristic can either be physical or behavioral characteristic; used for the person's recognition. Physical characteristics are characteristics that are genetically implied and possibly influenced by the environment (e.g. face, iris, retina, finger, vascular structure etc.).

Behavioral characteristics are characteristics that are gathered or learned during time (e.g. signature, gait, typing dynamics, voice features etc.). Biometric data are highly unique to each individual, easily obtainable non-intrusively, time invariant (no significant changes over a period of time) and distinguishable by humans without much special training [3]. Fuzzy logic is an area of research, which provides solutions to the problems of vagueness which departs from the all or nothing logic. It logically redefines yes or no ideas in proper form [4]. Lotfi Zadeh, while looking for an easier way to design complex control processes argued that in the real world we are commonly unable to define a clear and undeniable characteristic function stating whether or not an element belongs to a set.

Human reasoning is not only able to make decisions and classify situations based on partial or ambiguous information. Fuzzy logic is a good tool when dealing with uncertainty; can be a good measure of how close a decision is. The demand for reliable security system is increasing around the world, with the different types of biometrics traits; it is very important to choose the best among the biometrics traits for security enhancement. To determine the best among the biometrics characteristics, factors such as Universality, Uniqueness, Permanence, Collectability, Performance and Circumvention are evaluated against the biometrics traits using fuzzy logic. Based on the fact, this paper attempts to propose a holistic approach for evaluating biometric characteristics.

Lotfi A. Zadeh first used the term "fuzzy" in 1962, [5] he is often known as the father of fuzzy logic. Basically, fuzzy logic is a multi-valued logic that allows intermediate values to be defined between conventional evaluations like true/false, yes/no, high/low etc. [6]. Notions like rather tall or very fast can be formulated mathematically and processed by computers, in order to apply a more human-like way of thinking in the programming of computers [4]. Fuzzy system is an alternative to traditional notions of set membership and logic that has its origins in ancient Greek philosophy [6]. The values of system variables are not always known precisely rather approximately values are more likely to be known. This imprecise/uncertain nature of systems cannot be adequately represented/expressed using the classical set which is crisp in nature. The vagueness can adequately be handled using fuzzy set theory [5].

2. FUZZY SET THEORY

2.1 Fuzzy Set Union (OR)

The union of two Fuzzy Sets A and B defined over the same universe of discourse X is a new fuzzy set denoted as

$A \cup B$ with MF that represent the maximum degree of relevance between each element and the new Fuzzy Set [7]. The Fuzzy union operator is generally specified by a function, $S : [0,1] \times [0,1] \rightarrow [0,1]$. Symbolically,

$$\mu_{A \cup B}(x) = S(\mu_A(x), \mu_B(x)) = \mu_A(x) \hat{+} \mu_B(x) \quad (1)$$

Where $\hat{+}$ is a binary operator for the function S , this class of fuzzy union operators is referred to as *T-Conorm* (or *S-norm*) operator. It satisfies the following basic requirements:

$$S(1,1)=1, S(0,a)=S(a,0)=a \quad (\text{boundary})$$

$$S(a,b) \leq S(c,d) \text{ if } a \leq c \text{ and } b \leq d \quad (\text{monotonicity})$$

$$S(a,b)=S(b,a) \quad (\text{Commutativity})$$

$$S(a,S(b,c)) \leq S(S(a,b),c) \quad (\text{Associativity})$$

In fuzzy inference, fuzzy union is used to represent the “Or” operation.

2.2 Fuzzy Set Intersection (AND)

The intersection of two Fuzzy Sets A and B defined over the same Universe of discourse X , is a new Fuzzy set denoted as $A \cap B$ with MF that represent the minimum degree of relevance between each element and the new Fuzzy Set [8]. This intersection operator is generally specified by a function $T : [0,1] \times [0,1] \rightarrow [0,1]$, which aggregates the membership grades as follows:

$$\mu_{A \cap B}(x) = T(\mu_A(x), \mu_B(x)) = \mu_A(x) \otimes \mu_B(x) \quad (2)$$

Where $\otimes$ is a binary operator for the function T , this class of fuzzy intersection operators is referred to as *T-norm* (Triangular norm). It satisfies the following basic requirements:

$$T(0,0)=0, T(1,a)=T(a,1)=a \quad (\text{boundary})$$

$$T(a,b) \leq T(c,d) \text{ if } a \leq c \text{ and } b \leq d \quad (\text{monotonicity})$$

$$T(a,b)=T(b,a) \quad (\text{Commutativity})$$

$$T(a,T(b,c)) \leq T(T(a,b),c) \quad (\text{Associativity})$$

In fuzzy inference, intersection is used to represent the “and” operator [7].

2.3 Membership Functions (MF)

(f) Triangular MF

The Triangular MF is specified by three parameters $\{a,b,c\}$ as follows:

$$\text{triangle}(x : a, b, c) = \begin{cases} 0 & x \leq a \\ \frac{x-a}{b-a} & a \leq x \leq b \\ \frac{c-x}{c-b} & b \leq x \leq c \\ 0 & c \leq x \end{cases} \quad (3)$$

By using min and max, the above can be alternatively stated as:

$$\text{triangle}(x : a, b, c) = \max\left(\min\left(\frac{x-a}{b-a}, \frac{c-x}{c-b}\right), 0\right) \quad (4)$$

The parameters $\{a,b,c,d\}$ with $a < b < c$ determines the x coordinates of the three corners of the underlying triangle [9].

(g) Trapezoid MF

The Trapezoid MF is specified by four parameters $\{a,b,c,d\}$ as follows:

$$\text{trapezoid}(x : a, b, c, d) = \begin{cases} 0 & x \leq a \\ \frac{x-a}{b-a} & a \leq x \leq b \\ 1 & b \leq x \leq c \\ \frac{d-x}{d-c} & c \leq x \leq d \\ 0 & d \leq x \end{cases} \quad (5)$$

By using min and max, a concise expression of the above is

$$\text{trapezoidal}(x : a, b, c, d) = \max\left(\min\left(\frac{x-a}{b-a}, \frac{d-x}{d-c}\right), 0\right) \quad (2)$$

The parameters $\{a,b,c,d\}$ with $a < b \leq c < d$ determines the x coordinates of the four corners of the underlying trapezoid.

In real time implementation, the triangular MFs and the trapezoid MF have been used extensively due to their simple formulas and computational efficiency [9].

(h) Gaussian MFs

The Gaussian MF is specified by two parameters $\{c, \sigma\}$ and

$$gaussian(x : c, \sigma) = \ell^{-\frac{1}{2} \left(\frac{x-c}{\sigma} \right)^2} \quad (7)$$

Where c represents the MF center and σ determines the MF's width.

(i) Generalized Bell MF

This is known as Bell MF and it is specified by the three parameters $\{a, b, c\}$ [6].

$$bell(x : a, b, c) = \frac{1}{1 + \left| \frac{x-c}{a} \right|^{2b}} \quad (8)$$

Where the parameter b is usually positive. If b is negative the shape of the MF becomes an upside-down bell. Because of their smoothness and concise notation, Gaussian and bell Fuzzy control provides a formal methodology for representing, manipulating and implementing a human's heuristic knowledge about to control a system [5]. Figure 1 shows the block diagram of a Fuzzy controller embedded in

MFs are becoming increasingly popular for specifying fuzzy sets.

(j) Sigmoidal MFs

This is defined by

$$sig(x : a, c) = \frac{1}{1 + \exp[-a(x - c)]} \quad (9)$$

Where a controls the slope at the crossover point $x=c$. Figure ... depicts this MF. According to [9], depending on the sign of the parameter a , a sigmoidal MF is inherently open left or right and thus it is most appropriate for representing concept such as "very large" or "very negative".

3. METHODOLOGY

3.1 Fuzzy Control

a closed-loop control system. The systems outputs are denoted by $O(t)$, its input are denoted by $I(t)$ and the reference input to the fuzzy controller is denoted by $R(t)$.

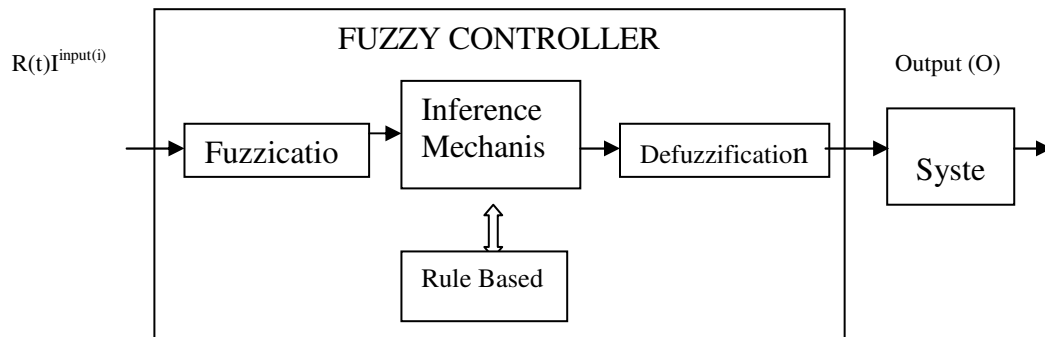


Figure 1: A block diagram of a fuzzy Controller

The Fuzzy Controller according to [10] is composed of the following elements:

- (e) A **Rule Based** (a set of **IF – THEN** rules): This contains a fuzzy logic quantification of an Expert's linguistic description of how to achieve good control. A Rule Base is said to be "complete" if for every possible combination of the inputs to the fuzzy system it can infer a response and generate an output. It is said to be "consistence" if there are no rules that have the same premise and different consequent.
- (f) An **Inference Mechanism**: This emulates the expert's decision making in interpreting and applying knowledge about how best to control the system.
- (g) A **Fuzzification Interface**: This converts controller inputs into information that the inference can easily use to activate and apply rules.
- (h) A **Defuzzification Interface**: This converts the conclusion of the inference mechanism into actual inputs for the system.

3.2 Factors of Biometrics Characteristics

The suitability of a physical or a behavioral trait is determined by seven factors which are used in a biometric application as identified by [11].

Table 1: Comparison of various biometric traits from [11][12].

Biometrics Traits	UV	UQ	PM	CL	PF	AC	CV
Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Hand Geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand Veins	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Retinal Scan	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H
Facial Thermograph	H	H	L	H	M	H	L
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M
PalmPrint	M	H	H	M	H	M	M

Before any human physiological or behavioral traits can be used as a biometric traits it must satisfies the following factors [12][11].

1. **Universality (UV):** Every individual must possess the characteristics. Each individual must have a biometric element that can be used for identification; there should be a way of accommodating people.
2. **Uniqueness (UQ):** Two people cannot be sufficiently equal in term of the characteristics. The biometric element must be distinctive to each person.
3. **Permanence (PM):** It measures how well a biometric resist aging. For each person, the property of the biometric element remains permanent over time.
4. **Collectability (CL):** The ease of acquisition or measurement of the trait. i.e. it must be easily collectible.
5. **Performance (PF):** it relates to the accuracy, speed and robustness of technology used. i.e. the method must deliver accurate results under varied environmental circumstances.
6. **Acceptability (AC):** it measures the degree of approval of a technology. i.e. the general public must accept the sample collection routines.
7. **Circumvention (CV):** it refers to the ease with which the trait of an individual can be imitated using artifacts. It measures the ease of use of a substitute.

3.3 Fuzzy System Block

The basic component of any fuzzy system is composed of:

- iv. Fuzzifier
- v. The inference engine
- vi. The Defuzzifier

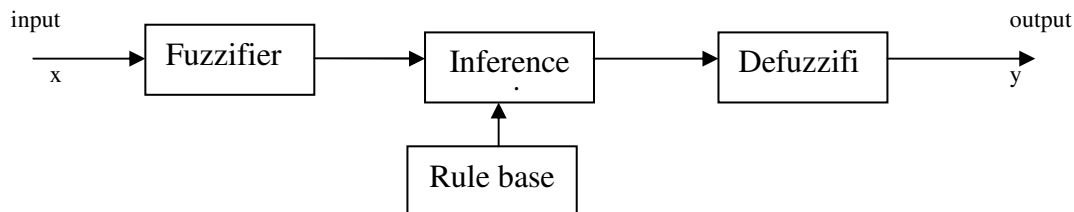


Figure 2: Block diagram of a fuzzy inference system.

The fuzzifier: This maps input numbers into corresponding fuzzy memberships. This is required in order to activate rules that are in terms of linguistic variables. The fuzzifier takes input values and determines the degree to which they belong to each of the fuzzy sets via membership functions.

The inference engine: This defines mapping from input fuzzy sets into output fuzzy sets. It determines the degree to which the antecedent is satisfied for each rule. If the antecedent of a given rule has more than one clause, fuzzy operators are applied to obtain one number that represents the result of the antecedent for that rule. It is possible that one or more rules may fire at the same time. Outputs for all rules are then aggregated. During aggregation, fuzzy sets that represent the output of each rule are combined into a single fuzzy set.

The defuzzifier: it maps output fuzzy sets into a crisp number. Given a fuzzy set that encompasses a range of output values, the defuzzifier.

3.4 Fuzzy Scale

According to [11] biometric traits are categorized using some factors like universality, uniqueness as mentioned earlier and each of these are indicated as Low, Medium or High (L, M, and H respectively). In applying fuzzy logic, three fuzzy sets are used in the comparison table. These are L, M and H which can be called the “security level”. Therefore, a scale of 0 to 5 to characterize the security level (L, M and H) is provided with each linguistic modifier having membership value from 0 to 1. The fuzzy linguistic variable “security” in this example represents security level. Scale with number 1 represents the highest level of low security with a membership value of 0.6, while scale number 2 defines low security with a membership value of 0.2 or average performance with membership value of 0.4. This implies that scale number 3 describes security level that is 80% average and 20% low. The three fuzzy sets are as follow:

Low_security = {0|1.0, 0.5|0.8, 1.0|0.6, 1.5|0.4, 2.0|0.2, 2.5|0.0, 3.0|0.0, 3.5|0.0, 4.0|0.0, 4.5|0.0, 5.0|0.0}

Medium_security = {0|0.0, 0.5|0.0, 1.0|0.0, 1.5|0.2, 2.0|0.4, 2.5|0.6, 3.0|0.8, 3.5|1.0, 4.0|0.0, 4.5|0.0, 5.0|0.0}

High_security = {0|0.0, 0.5|0.0, 1.0|0.0, 1.5|0.0, 2.0|0.0, 2.5|0.0, 3.0|0.2, 3.5|0.4, 4.0|0.6, 4.5|0.8, 5.0|1.0}

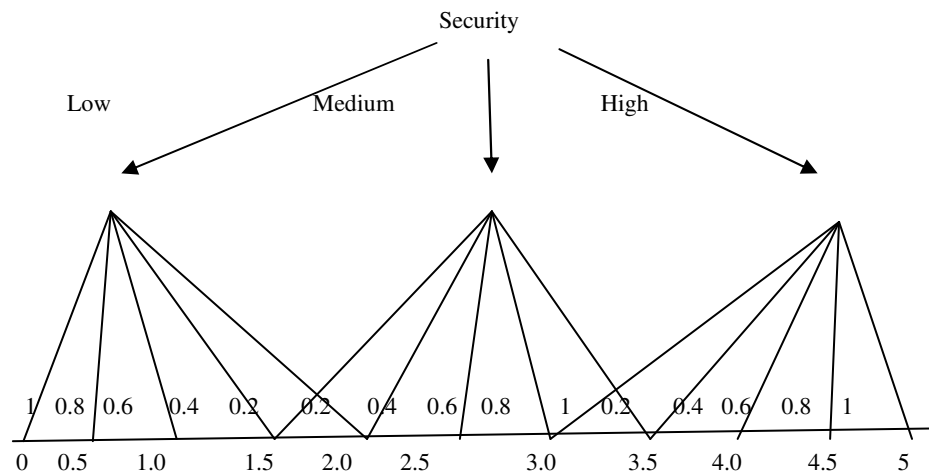


Figure 3: Three fuzzy sets for security rating.

3.5 Fuzzy Evaluation

The paper uses principles of fuzzy logic to analysis or evaluation the categorized biometrics traits according to [11] as shown in table 1.

A fuzzy set C is formed which takes values in a universe of discourse U in the interval of $[0, 1]$ [13] such that:

$$C = \{u | f_C(u), u \in U\} \quad (10)$$

Table 2: Factor of each biometric trait and their membership grades (MG).

Factors	Representation(U)	Membership Grades $f_C(U)$
Universality	a1	1
Uniqueness	a2	0.9
Permanence	a3	0.7
Collectability	a4	0.6
Performance	a5	0.5
Circumvention	a6	0.3

This table assigned a membership grade between 0 to 1 for factor satisfied for each biometrics traits. Therefore, each factor is given a qualitative judgment to determine the level of security for the selected factor category.

$f_C(U) = \{1.0, 0.9, 0.7, 0.6, 0.5, 0.3\}$ as shown in table 2.

Table 3: Linguistic variables employed for (a1, a2, a3, a4 and a5) decision making.

Membership Grade	Linguistic variables	Representation
0.1	Very Low	VL
0.3	Low	L
0.6	Medium	M
0.9	High	H
1.0	Very High	VH

Table 4: Linguistic variables employed for (a6: Circumvention) decision making.

Membership Grade	Linguistic variables	Representation
0.3	Easily Fake	H
0.6	Averagely Fake	M
0.9	Not Easily Fake	L

These Linguistic variables therefore formed another fuzzy set and denoted with letter E , which takes values in a universe of discourse U (i.e factor) in the interval of [0, 1] [13][14] such that [13][14]:

$$E = \{U | f_E(U), u \in U\} \quad (11)$$

$$f_E(U) = \{0.1, 0.3, 0.6, 0.9, 1.0\}$$

3.6 The Inference Engine

Next is to assess the security level of each biometric trait by each factor that is based on the fuzzy opinion of the decision maker. This decision brings about fifteen (15) different fuzzy sets as shown in table 5. This is denoted as: $E1, E2, E3, \dots, E15$ with membership functions: $f_{E1}(U), f_{E2}(U), f_{E3}(U), \dots, f_{E15}(U)$ respectively. From this table, B denotes biometric traits and A for factors. However, fuzzy logic approach is used to provide a reasonable solution for the evaluation of the best among the biometric traits in terms of security level.

Therefore, the fuzzy sets and membership of the biometric traits (B) are as follows:

$$E1 = \{1.0|0.9, 2.0|0.3, 3.0|0.6, 4.0|0.9, 5.0|0.3, 6.0|0.3\}$$

$$f_{E1}(U) = \{0.9, 0.3, 0.6, 0.9, 0.3, 0.3\}$$

$$E2 = \{1.0|0.6, 2.0|0.9, 3.0|0.9, 4.0|0.6, 5.0|0.9, 6.0|0.6\}$$

$$f_{E2}(U) = \{0.6, 0.9, 0.9, 0.6, 0.9, 0.6\}$$

$$E3 = \{1.0|0.6, 2.0|0.6, 3.0|0.6, 4.0|0.9, 5.0|0.6, 6.0|0.6\}$$

$$f_{E3}(U) = \{0.6, 0.6, 0.6, 0.9, 0.6, 0.6\}$$

$E4 = \{1.0|0.3, 2.0|0.3, 3.0|0.3, 4.0|0.6, 5.0|0.3, 6.0|0.6\}$
 $fE4(U) = \{0.3, 0.3, 0.3, 0.6, 0.3, 0.6\}$
 $E5 = \{1.0|0.6, 2.0|0.6, 3.0|0.6, 4.0|0.6, 5.0|0.6, 6.0|0.9\}$
 $fE5(U) = \{0.6, 0.6, 0.6, 0.6, 0.6, 0.9\}$
 $E6 = \{1.0|0.9, 2.0|0.9, 3.0|0.9, 4.0|0.6, 5.0|0.9, 6.0|0.9\}$
 $fE6(U) = \{0.9, 0.9, 0.9, 0.6, 0.9, 0.9\}$
 $E7 = \{1.0|0.9, 2.0|0.9, 3.0|0.6, 4.0|0.3, 5.0|0.9, 6.0|0.9\}$
 $fE7(U) = \{0.9, 0.9, 0.6, 0.3, 0.9, 0.9\}$
 $E8 = \{1.0|0.3, 2.0|0.3, 3.0|0.3, 4.0|0.9, 5.0|0.3, 6.0|0.3\}$
 $fE8(U) = \{0.3, 0.3, 0.3, 0.9, 0.3, 0.3\}$
 $E9 = \{1.0|0.6, 2.0|0.3, 3.0|0.3, 4.0|0.6, 5.0|0.3, 6.0|0.3\}$
 $fE9(U) = \{0.6, 0.3, 0.3, 0.6, 0.3, 0.3\}$
 $E10 = \{1.0|0.9, 2.0|0.9, 3.0|0.3, 4.0|0.9, 5.0|0.6, 6.0|0.9\}$
 $fE10(U) = \{0.9, 0.9, 0.3, 0.9, 0.6, 0.9\}$
 $E11 = \{1.0|0.9, 2.0|0.9, 3.0|0.9, 4.0|0.3, 5.0|0.3, 6.0|0.9\}$
 $fE11(U) = \{0.9, 0.9, 0.9, 0.3, 0.3, 0.9\}$
 $E12 = \{1.0|0.9, 2.0|0.9, 3.0|0.9, 4.0|0.3, 5.0|0.9, 6.0|0.9\}$
 $fE12(U) = \{0.9, 0.9, 0.9, 0.3, 0.9, 0.9\}$
 $E13 = \{1.0|0.6, 2.0|0.3, 3.0|0.3, 4.0|0.9, 5.0|0.3, 6.0|0.6\}$
 $fE13(U) = \{0.6, 0.3, 0.3, 0.9, 0.3, 0.6\}$
 $E14 = \{1.0|0.6, 2.0|0.6, 3.0|0.9, 4.0|0.6, 5.0|0.6, 6.0|0.6\}$
 $fE14(U) = \{0.6, 0.6, 0.9, 0.6, 0.6, 0.6\}$
 $E15 = \{1.0|0.6, 2.0|0.9, 3.0|0.9, 4.0|0.6, 5.0|0.9, 6.0|0.6\}$
 $fE15(U) = \{0.6, 0.9, 0.9, 0.6, 0.9, 0.6\}$

Table 5: Factors across biometric traits

	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15
a1	0.9	0.6	0.6	0.3	0.6	0.9	0.9	0.3	0.6	0.9	0.9	0.9	0.6	0.6	0.6
a2	0.3	0.9	0.6	0.3	0.6	0.9	0.9	0.3	0.3	0.9	0.9	0.9	0.3	0.6	0.9
a3	0.6	0.9	0.6	0.3	0.6	0.9	0.6	0.3	0.3	0.3	0.9	0.9	0.3	0.9	0.9
a4	0.9	0.6	0.9	0.6	0.6	0.6	0.3	0.9	0.6	0.9	0.3	0.3	0.9	0.6	0.6
a5	0.3	0.9	0.6	0.3	0.6	0.9	0.9	0.3	0.3	0.6	0.3	0.9	0.3	0.6	0.9
a6	0.3	0.6	0.6	0.6	0.9	0.9	0.9	0.3	0.3	0.9	0.9	0.9	0.6	0.6	0.6

3.7 Fuzzy Implication

Now, fuzzy implication is established between a specific factor and security level of biometric traits. This can be done by finding the complement of the factor which will give a minimum security value assigned to all the biometric traits.

Recall, factor fuzzy set is: $fC(U) = \{1.0, 0.9, 0.7, 0.6, 0.5, 0.3\}$

So, complement for factor fuzzy set will be:

$$\begin{aligned}
 f_{\neg C}(U) &= 1 - \{1.0, 0.9, 0.7, 0.6, 0.5, 0.3\} \\
 &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\}
 \end{aligned}$$

The Max function is then applied to all the biometric trait fuzzy sets and the complement of the factor set as shown below:

$$\begin{aligned}
 f_{\neg C \vee E1}(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.9, 0.3, 0.6, 0.9, 0.3, 0.3\} \\
 &= \{0.9, 0.3, 0.6, 0.9, 0.3, 0.3\} \\
 f_{\neg C \vee E2}(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.6, 0.9, 0.9, 0.6, 0.9, 0.6\} \\
 &= \{0.6, 0.9, 0.9, 0.6, 0.9, 0.6\}
 \end{aligned}$$

$$\begin{aligned}
 f_{\neg C} VE3(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.6, 0.6, 0.6, 0.9, 0.6, 0.6\} \\
 &= \{0.6, 0.6, 0.6, 0.9, 0.6, 0.6\} \\
 f_{\neg C} VE4(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.3, 0.3, 0.3, 0.6, 0.3, 0.6\} \\
 &= \{0.3, 0.3, 0.3, 0.6, 0.3, 0.6\} \\
 f_{\neg C} VE5(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.6, 0.6, 0.6, 0.6, 0.6, 0.9\} \\
 &= \{0.6, 0.6, 0.6, 0.6, 0.6, 0.9\} \\
 f_{\neg C} VE6(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.9, 0.9, 0.9, 0.6, 0.9, 0.9\} \\
 &= \{0.9, 0.9, 0.9, 0.6, 0.9, 0.9\} \\
 f_{\neg C} VE7(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.9, 0.9, 0.6, 0.3, 0.9, 0.9\} \\
 &= \{0.9, 0.9, 0.6, 0.3, 0.9, 0.9\} \\
 f_{\neg C} VE8(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.3, 0.3, 0.3, 0.9, 0.3, 0.3\} \\
 &= \{0.3, 0.3, 0.3, 0.9, 0.3, 0.3\} \\
 f_{\neg C} VE9(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.6, 0.3, 0.3, 0.6, 0.3, 0.3\} \\
 &= \{0.6, 0.3, 0.3, 0.6, 0.3, 0.3\} \\
 f_{\neg C} VE10(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.9, 0.9, 0.3, 0.9, 0.6, 0.9\} \\
 &= \{0.9, 0.9, 0.3, 0.9, 0.6, 0.9\} \\
 f_{\neg C} VE11(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.9, 0.9, 0.9, 0.3, 0.3, 0.9\} \\
 &= \{0.9, 0.9, 0.9, 0.3, 0.3, 0.9\} \\
 f_{\neg C} VE12(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.9, 0.9, 0.9, 0.3, 0.9, 0.9\} \\
 &= \{0.9, 0.9, 0.9, 0.3, 0.9, 0.9\} \\
 f_{\neg C} VE13(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.6, 0.3, 0.3, 0.9, 0.3, 0.6\} \\
 &= \{0.6, 0.3, 0.3, 0.9, 0.3, 0.6\} \\
 f_{\neg C} VE14(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.6, 0.6, 0.9, 0.6, 0.6, 0.6\} \\
 &= \{0.6, 0.6, 0.9, 0.6, 0.6, 0.6\} \\
 f_{\neg C} VE15(U) &= \{0.0, 0.1, 0.3, 0.4, 0.5, 0.7\} \vee \{0.6, 0.9, 0.9, 0.6, 0.9, 0.6\} \\
 &= \{0.6, 0.9, 0.9, 0.6, 0.9, 0.6\}
 \end{aligned}$$

3.8 The Defuzzifier

Finally, Min function is applied to the sets derived for each biometric trait in the fuzzy set union operation above in order to arrive at the final evaluation; the model generated various security levels of each biometric trait which can be seen in the table 6:

Table 6: Overall numerical security level across biometric traits

BIOMETRIC TRAITS	SECURITY LEVEL
E1	0.3
E2	0.6
E3	0.6
E4	0.3
E5	0.6
E6	0.6
E7	0.3
E8	0.3
E9	0.3
E10	0.3
E11	0.3
E12	0.3
E13	0.3
E14	0.6
E15	0.6

4. RESULTS AND DISCUSSION

Table 7 shows the summary of the result of overall evaluation of security level of Biometric traits using [11] biometric traits comparison. The result in the table shows that security level of E2, E3, E5, E6 E14 and E15 is 60%, which indicates a Medium security level while other biometric traits are with 30%, which implies a Low security level.

Table 7: Overall security level of Biometric traits

BIOMETRIC TRAITS	SECURITY LEVEL
Face (E1)	Low
Fingerprint (E2)	Medium
Hand Geometry (E3)	Medium
Keystrokes (E4)	Low
Hand Veins (E5)	Medium
Iris (E6)	Medium
Retinal Scan (E7)	Low
Signature (E8)	Low
Voice (E9)	Low
Facial Thermograph (E10)	Low
Odor (E11)	Low
DNA (E12)	Low
Gait (E13)	Low
Ear Canal (E14)	Medium
PalmPrint (E15)	Medium

The proposed fuzzy logic approach was simulated using Qtfuzzylite 4.0 (A Fuzzy Logic Control Library in C++) to test the performance of the model. Figure 4 shows the interface for settings for all the fifteen (15) Biometrics traits. On the range of 0 – 15; each point represent biometric trait such as 1 for Face, 2 for Fingerprint and so on.

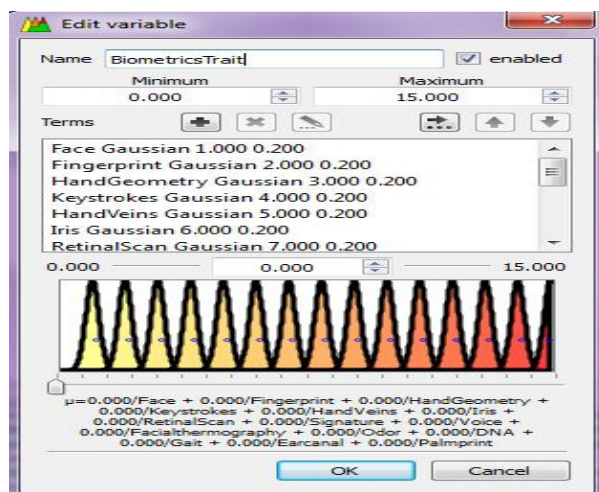


Figure 4: Biometrics Traits settings

The membership grade for factors a1, a2, a3, a4 and a5 is defined on the scale of 0.3 for Low, 0.6 for Medium and 0.9 for High as shown in Figure 5 while that of Circumvention (a6) is shown in Figure 6 defined on the scale of 0.3 for High, 0.6 for Medium and 0.9 for Low.

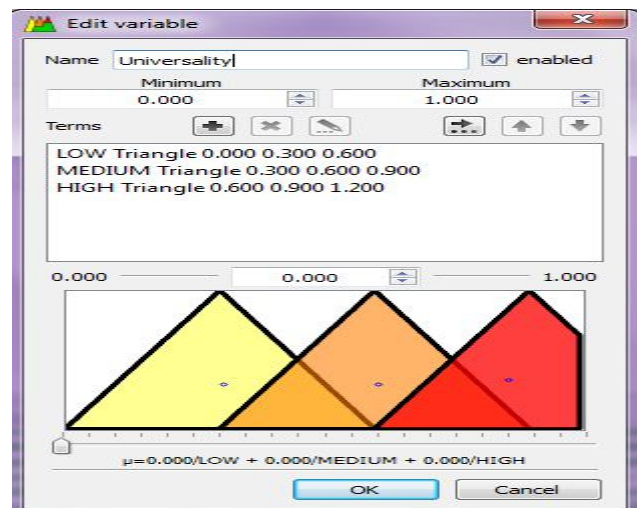


Figure 5: Membership Grade for a1 - a5

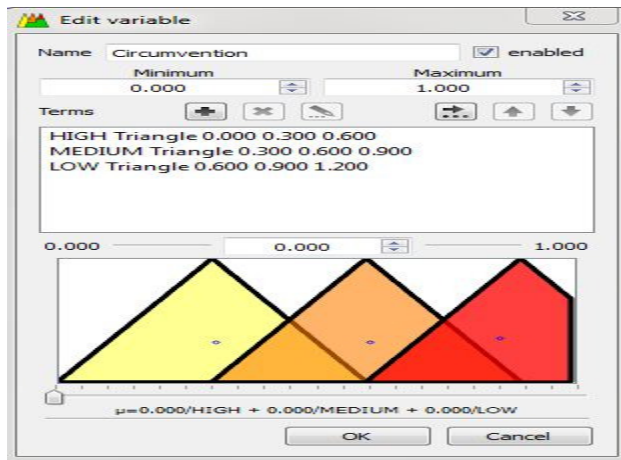


Figure 6: Membership Grade for Circumvention

The Security level has a membership grade on the scale of 0.3 for Low, 0.6 for Medium and 0.9 for High. The type of Defuzzifier is declared as Mean of Maximum while the Accumulation is declared as Maximum as shown in Figure 7.

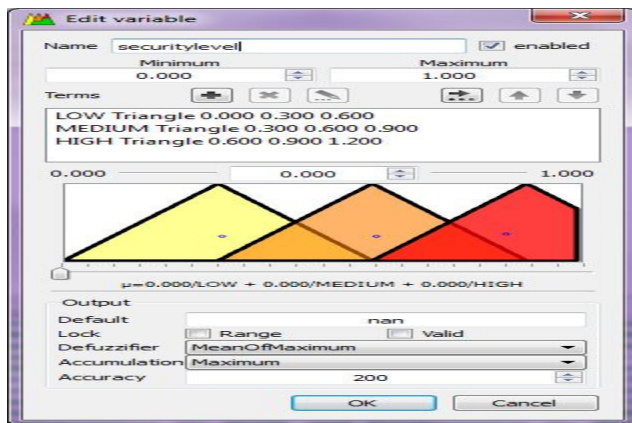


Figure 7: Membership Grade for Security level

During the simulation, Face biometrics has a deterministic rule: if Biometric is Face and Universality is HIGH and Uniqueness is LOW and Permanence is MEDIUM and Collectability is HIGH and Performance is LOW and Circumvention is HIGH then SecurityLevel is LOW. As seen in Figure 8, the result shows that SecurityLevel is LOW with a green triangle and an indicator at the middle of it, which indicate the point 0.3.



Figure 8: Simulation of Face biometric

Fingerprint biometric has a deterministic rule: if Biometric is Fingerprint and Universality is MEDIUM and Uniqueness is HIGH and Permanence is HIGH and Collectability is MEDIUM and Performance is HIGH and Circumvention is MEDIUM then SecurityLevel is MEDIUM. As seen in Figure 9, the result shows that SecurityLevel is MEDIUM with a green triangle and an indicator at the middle of it, which indicate the point 0.6.

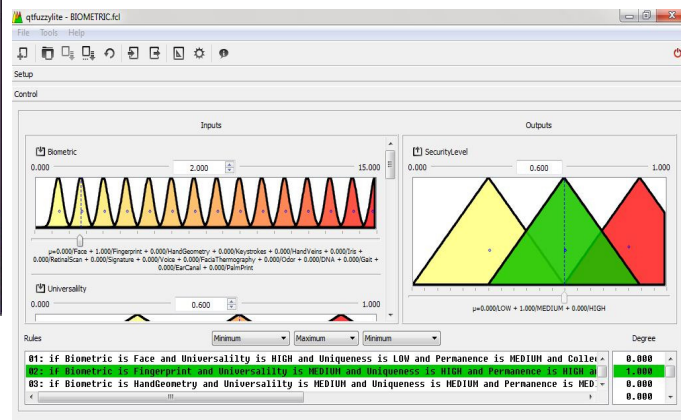


Figure 9: Simulation of Fingerprint biometric

Hand Geometry biometric has a deterministic rule: if Biometric is HandGeometry and Universality is MEDIUM and Uniqueness is MEDIUM and Permanence is MEDIUM and Collectability is HIGH and Performance is MEDIUM and Circumvention is MEDIUM then SecurityLevel is MEDIUM. As seen in Figure 10, the result shows that SecurityLevel is MEDIUM with a green triangle and an indicator at the middle of it which indicate the point 0.6.

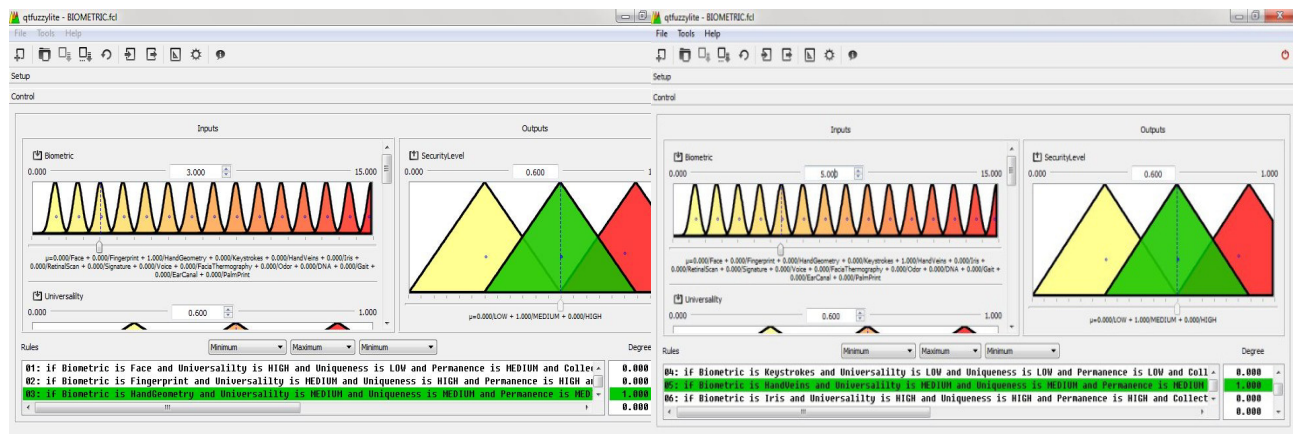


Figure 11: Simulation of Hand Geometry biometric

Keystrokes biometric has a deterministic rule: if Biometric is Keystrokes and Universality is LOW and Uniqueness is LOW and Permanence is LOW and Collectability is MEDIUM and Performance is LOW and Circumvention is MEDIUM then SecurityLevel is LOW. As seen in Figure 12, the result shows that SecurityLevel is LOW with a green triangle and an indicator at the middle of it which indicate the point 0.3.

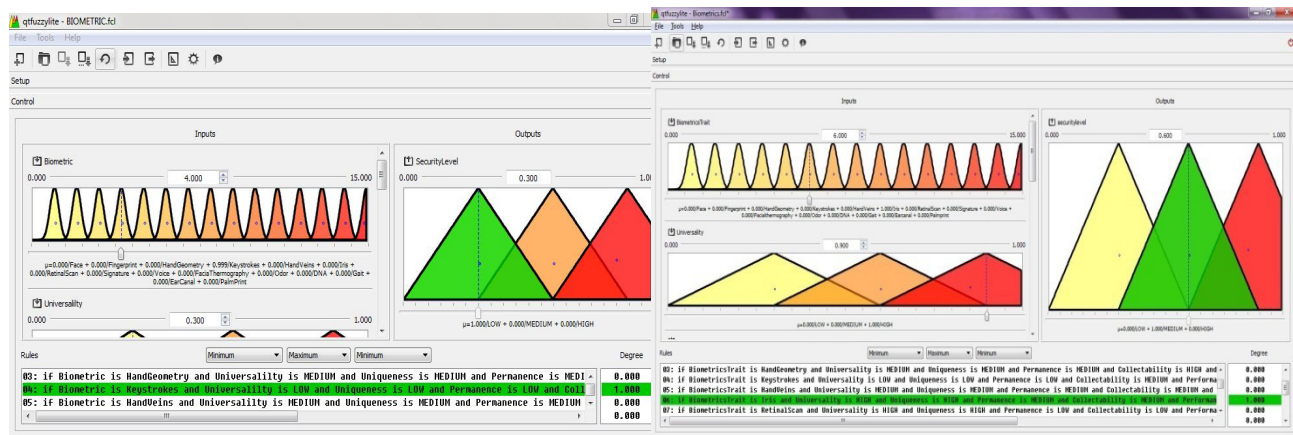


Figure 12: Simulation of Keystrokes biometric

Hand Veins biometric has a deterministic rule: if Biometric is HandVeins and Universality is MEDIUM and Uniqueness is MEDIUM and Permanence is MEDIUM and Collectability is LOW then SecurityLevel is MEDIUM. As seen in Figure 13, the result shows that SecurityLevel is MEDIUM with a green triangle and an indicator at the middle of it which indicate the point 0.6.

Iris biometric biometric has a deterministic rule: if Biometric is Iris and Universality is HIGH and Uniqueness is HIGH and Permanence is HIGH and Collectability is MEDIUM and Performance is HIGH and Circumvention is LOW then SecurityLevel is MEDIUM. As seen in Figure 14, the result shows that SecurityLevel is MEDIUM with a green triangle and an indicator at the middle of it which indicate the point 0.6.

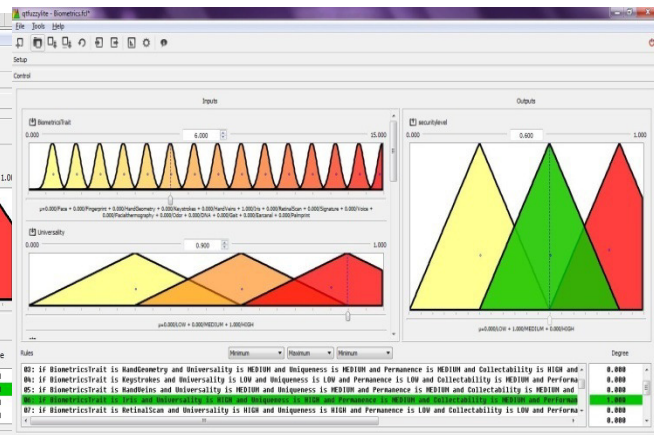


Figure 13: Simulation of Hand Veins biometric

Retinal Scan biometric has a deterministic rule: if Biometric is RetinalScan and Universality is HIGH and Uniqueness is HIGH and Permanence is MEDIUM and Collectability is LOW and Performance is HIGH and Circumvention is LOW then SecurityLevel is LOW. As seen in Figure 15, the result shows that SecurityLevel is LOW with a green triangle and an indicator at the middle of it which indicate the point 0.3.

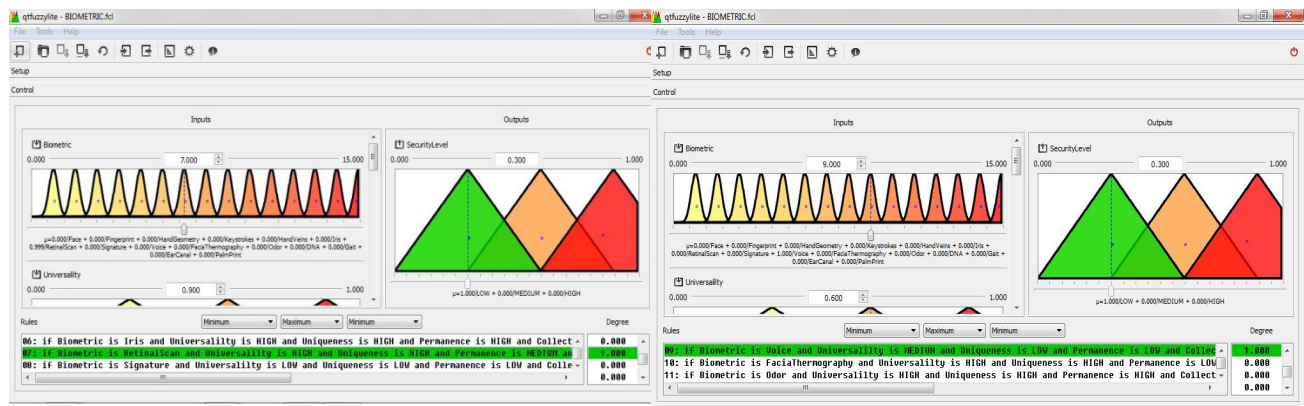


Figure 15: Simulation of Retinal Scan biometric

Signature biometric has a deterministic rule: if Biometric is Signature and Universality is LOW and Uniqueness is LOW and Permanence is LOW and Collectability is HIGH and Performance is LOW and Circumvention is HIGH then SecurityLevel is LOW. As seen in Figure 16, the result shows that SecurityLevel is LOW with a green triangle and an indicator at the middle of it which indicate the point 0.3.

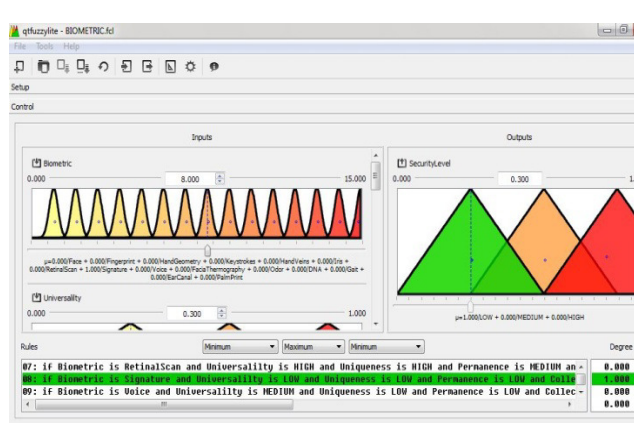


Figure 16: Simulation of Signature biometric

Voice biometric has a deterministic rule: if Biometric is Voice and Universality is MEDIUM and Uniqueness is LOW and Permanence is LOW and Collectability is MEDIUM and Performance is LOW and Circumvention is HIGH then SecurityLevel is LOW. As seen in Figure 17, the result shows that SecurityLevel is LOW with a green triangle and an indicator at the middle of it which indicate the point 0.3.

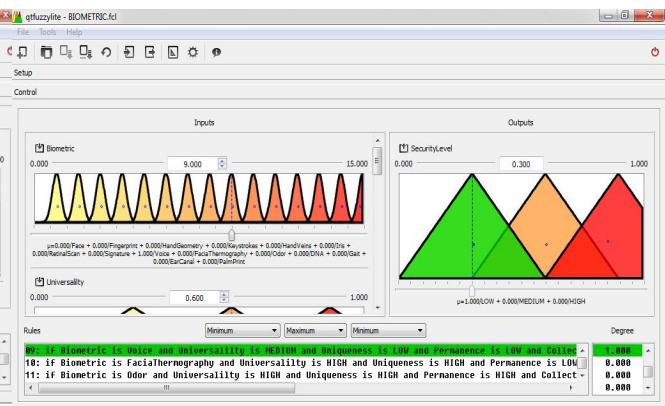


Figure 17: Simulation of Voice biometric

Facial thermograph biometric has a deterministic rule: if Biometric is FaciaThermography and Universality is HIGH and Uniqueness is HIGH and Permanence is LOW and Collectability is HIGH and Performance is MEDIUM and Circumvention is LOW then SecurityLevel is LOW. As seen in Figure 18, the result shows that SecurityLevel is LOW with a green triangle and an indicator at the middle of it which indicate the point 0.3.

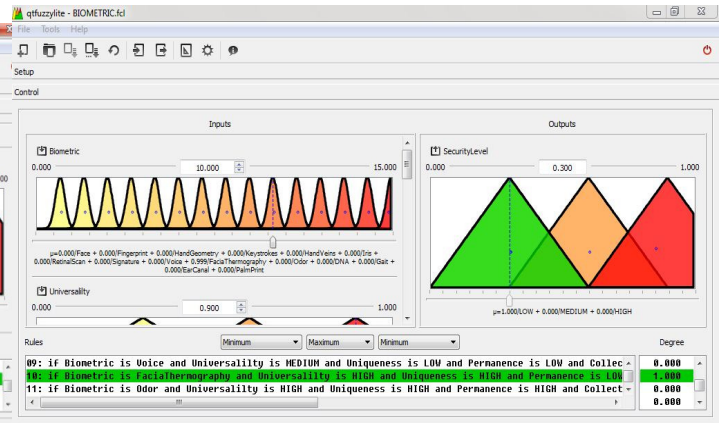


Figure 18: Simulation of Facial thermograph biometric

Odor biometric has a deterministic rule: if Biometric is Odor and Universality is HIGH and Uniqueness is HIGH and Permanence is HIGH and Collectability is LOW and Performance is LOW and Circumvention is LOW then SecurityLevel is LOW. As seen in Figure 19, the result shows that SecurityLevel is LOW with a green triangle and an indicator at the middle of it which indicate the point 0.3.

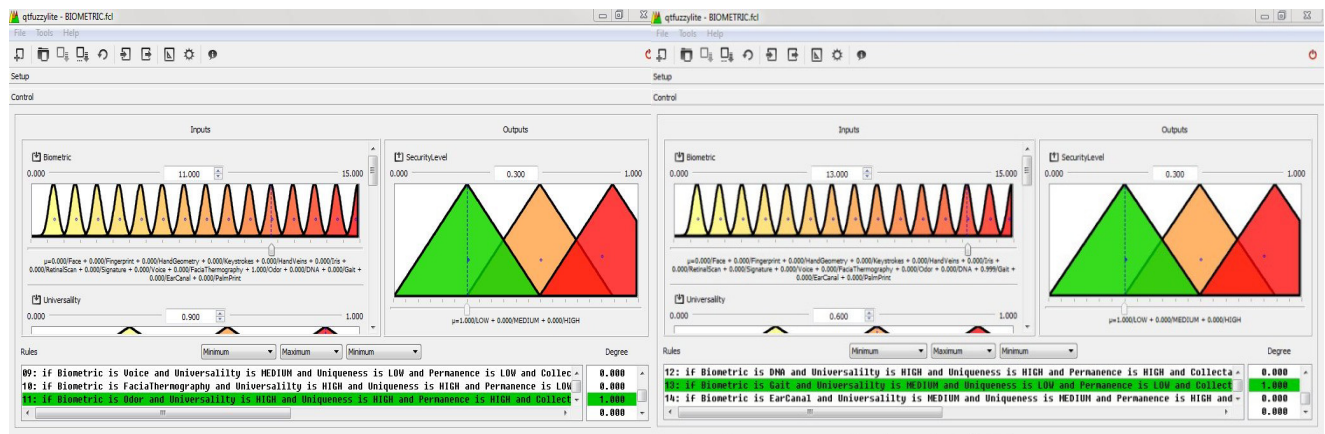


Figure 19: Simulation of Odor biometric

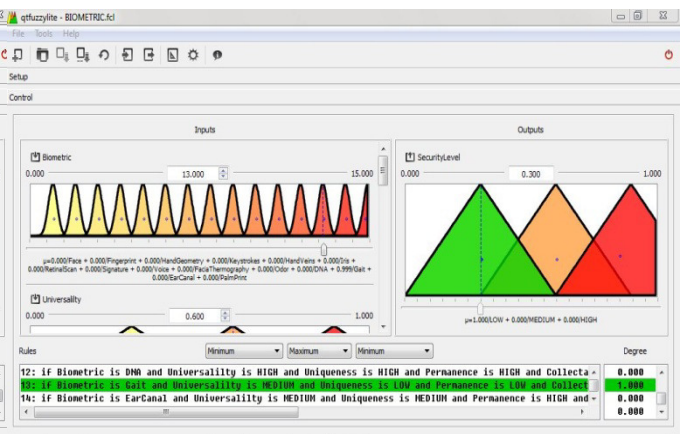


Figure 21: Simulation of Gait biometric

DNA biometric has a deterministic rule: if Biometric is DNA and Universality is HIGH and Uniqueness is HIGH and Permanence is HIGH and Collectability is LOW and Performance is HIGH and Circumvention is LOW then SecurityLevel is LOW. As seen in Figure 20, the result shows that SecurityLevel is LOW with a green triangle and an indicator at the middle of it which indicate the point 0.3.

Ear Canal biometric has a deterministic rule: if Biometric is EarCanal and Universality is MEDIUM and Uniqueness is MEDIUM and Permanence is HIGH and Collectability is MEDIUM and Performance is MEDIUM and Circumvention is MEDIUM then SecurityLevel is MEDIUM. As seen in Figure 22, the result shows that SecurityLevel is MEDIUM with a green triangle and an indicator at the middle of it which indicate the point 0.6.

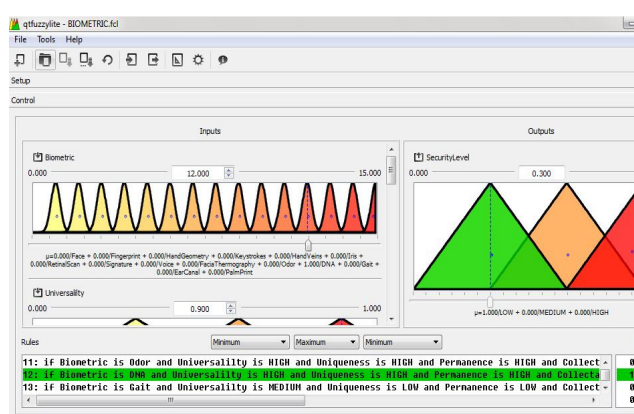


Figure 20: Simulation of DNA biometric

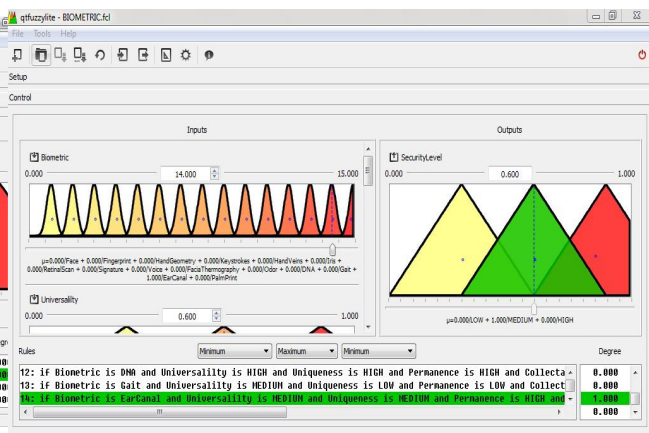


Figure 22: Simulation of Ear Canal biometric

Gait biometric has a deterministic rule: if Biometric is Gait and Universality is MEDIUM and Uniqueness is LOW and Permanence is LOW and Collectability is HIGH and Performance is LOW and Circumvention is MEDIUM then SecurityLevel is LOW. As seen in Figure 21, the result shows that SecurityLevel is LOW with a green triangle and an indicator at the middle of it which indicate the point 0.3.

Palmprint biometric has a deterministic rule: if Biometric is PalmPrint and Universality is MEDIUM and Uniqueness is HIGH and Permanence is HIGH and Collectability is MEDIUM and Performance is HIGH and Circumvention is MEDIUM then SecurityLevel is MEDIUM. As seen in Figure 23, the result shows that SecurityLevel is MEDIUM with a green triangle and an indicator at the middle of it which indicate the point 0.6.

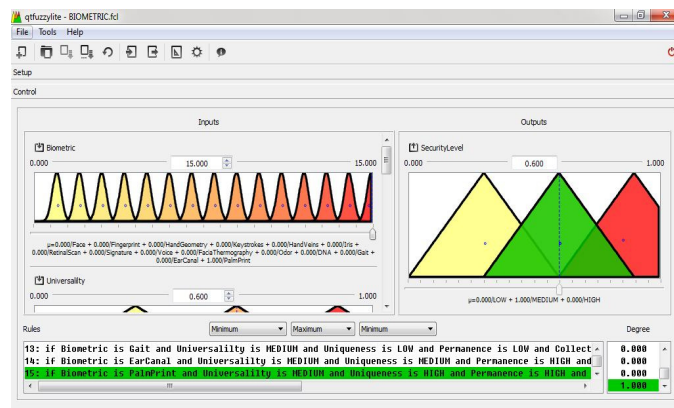


Figure 23: Simulation of Palmprint biometric

5. CONCLUSION

This paper revealed the applicability of fuzzy logic model to determine the security level of fifteen (15) Biometric traits considered in this research. Biometrics characteristics knowledge base categorized by the previous researchers in the field of Biometrics was used to develop a model that can be used to determine the security level of the various Biometric traits. The proposed model was simulated in Qtfuzzylite environment in order to test its applicability. In this evaluation, six (6) factors were considered which are Universality, Uniqueness, Permanence, Collectability, Performance and Circumvention and the results show that Fingerprint, Hand Geometry, Hand Veins, Iris, Ear Canal and Palm print have medium security level among the fifteen (15) Biometrics traits considered for evaluation. This model therefore, gives the decision maker a clear and flexible method of evaluation.

REFERENCES

- [1] Jimoh, R. G., Abdulsalam, S.O. and Adewole, K.S. "Adoption of Fingerprinting as an Automated Access Control Technique in University Hostels". *ARPJ Journal of Systems and Software*, 1(4), 2011, pp. 149-153.
- [2] Security Products; Security Management Solution, Retrieved 21th October, 2013 from www.self-safety.com/security-products/security-products-security-management-solutions.
- [3] Jain, K., Bolle, R., and Pankanti, S. Biometrics: Personal Identification in Networked Society. Norwell, MA: Kluwer Academy Publishers, 1999. ISBN 978-0792383451.
- [4] Zadeh, L.A. A Fuzzy set theoretical Approach to the compositionary of meaning, 1963.
- [5] Bajeh, O. A. and Emuoyibofarhe, O. J. A Fuzzy Logic Temperature Controller for Preterm Neonate Incubator. Proceedings of the first International Conference on Mobile Computing, Wireless

Communication, E-Health, M-Health and Telemedicine, 2008

- [6] Hellman, M. Fuzzy Logic introduction, 2001
- [7] Cirstea, M. N., Dina, A., Khor, J. G. and McCormick, M. Neural and Fuzzy Logic control of Drives and Power, Elsevier Science, 2002
- [8] Padhy, N. Artificial Intelligence and Intelligence Systems. New York: Oxford University Press, 2006
- [9] Jang, J., Sun, C. and Mizutani, E. Neuro-Fuzzy and soft computing (A computational Approach to learning and machine intelligence), Prentice Hall, 1997
- [10] Passino, K., Yurkovich, S. Fuzzy control. Addison Wesley Longman Inc. California, 1998
- [11] Jain, A.K, Ross, A. and Prabhakar, S. An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 2004, pp. 4-19.
- [12] Abikoye O.C. "An enhance Iris recognition system for personal authentication," Ph.D. thesis, Dept. Comp. Sci., University of Ilorin., Ilorin, Kwara, 2013.
- [13] Adewole, K.S., Ajiboye, A.R., Isiaka, R.M and Babatunde, R.S. A Fuzzy Logic Approach for Evaluation of Government Performance in ICT Projects Implementation. *Journal of Emerging Trends in Computing and Information Sciences*, 3(11), 2012, pp: 1487-1494.
- [14] Linguistic Variables, Values, and Rules. Retrieved 21st October, 2013 from www.6.zzu.edu.cn/shili/jxzy/ICtrl/text/chapter2/section3/2.3.1.htm