# An Exploratory Study Of Odor Biometrics Modality For Human Recognition

[1]Oyeleye, C. A., [2]Fagbola T. M, [3]Babatunde R. S, [4]Adigun A. A

*[1,2,4]Department of Computer Engineering and Technology, Ladoke Akintola University of Technology, Ogbomoso, Oyo State.*
*[3]Department of Computer, Library and Information Science, Kwara State University, Malete, Kwara State.*

## ABSTRACT

*The currently recurring and alarming global security challenges have led to the development and use of biometric modalities for access control and human recognition. Though a number of biometrics have been proposed, researched and evaluated for human recognition and access control applications; it becomes evident that each biometrics has its strengths and limitations as each best fit to a particular identification / security application. Thus, there is not one biometric modality that is perfect for all implementations. This opens a wide gap for the introduction and application of some newly emerging biometric modalities for human recognition. However, in security systems, biometrics commonly implemented or studied include fingerprint, face, iris, voice, signature and hand geometry. Whereas, a number of newly emerging biometric modalities including Gait, Vein, DNA, Body Odor, Ear Pattern, Keystroke and Lip, promising to provide better result in terms of performance, acceptability and circumvention are less studied, understood, researched or implemented for security applications. Body odor is one of the physical characteristics of a human that can be used to identify people. While body odor, which significantly exhibits strong security potentials over other recently emerging modalities, could prove very effective for accurate personal identification, little is known about its fundamental features and suitability for human recognition. Sequel to this, this paper carries out an exploratory study of odor biometrics modality for human recognition.*

**Keywords:** Odor biometrics, Human recognition

## 1. Introduction

Biometrics is the science of measuring physical properties of living beings [4]. It can be defined as any measurable, robust, distinctive physical characteristic or personal trait that can be used to identify, or verify the claimed identity of, an individual [2]. However, a biometric template is a digital representation of an individual's distinct characteristics, representing information extracted from a biometric sample. Biometric templates are what are actually compared in a biometric recognition system.

Biometrics are being used in many locations to enhance the security and convenience of the society. Biometrics commonly implemented or studied include fingerprint, face, iris, voice, signature and hand geometry. Other biometric strategies are being developed like those based on gait, retina, hand veins, ear canal, facial thermo gram, DNA, odor and palm prints [4]. Though, a number of biometric modalities have been well studied, little is known about odor biometric system. An odor is caused by one or more volatilized chemical compounds, generally at a very low concentration, that humans or other animals perceive by the sense of olfaction [1].

The body odor biometrics is based on the fact that virtually each human smell is unique. The smell is captured by sensors that are capable to obtain the odor from non-intrusive parts of the body such as the back of the hand or armpit [1].

Body odor recognition is a contactless physical biometric that attempts to confirm a person's identity by analyzing the olfactory properties of the human body scent [2]. Odor biometric system has been identified by a number of researchers as a viable system for personal identification [3]. The evaluation of odor characteristics and features is an important step to implementing odor as a personal identification and security system. In this paper, an exploratory study of odor biometric modality for human recognition is investigated and presented. It is organized as follows: section 2 discusses the biometrics for human recognition; section 3 explicitly examines the human body odor and associated issues while conclusion is drawn in section 4.

## 2. Biometrics for Human Recognition

The increased need of privacy and security in our daily life has given birth to this new area of science and technology [4]. Biometrics involves a set of approaches for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, biometrics is used as a form of identity access management and control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to identify individuals [5]. The two categories of biometric identifiers include physiological and behavioral characteristics [6]. Physiological characteristics are related to the shape of the body and include but are not limited to: fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition, and odor. However, behavioral characteristics are related to the behavior of a person, including but not limited to: typing rhythm, gait and voice. Biometrics works by unobtrusively matching patterns of live individuals in real time against enrolled records. Leading examples are biometric technologies that recognize and authenticate faces, hands, fingers, signatures, irises, voices and fingerprints

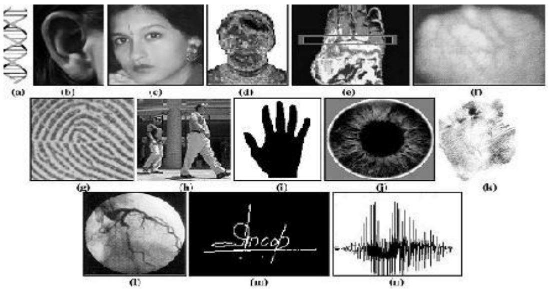

Fig.1: Examples of Various Biometric Characteristics: (a) DNA, (b) Ear,(c) Face, (d) Facial Thermogram, (e) Hand Thermogram, (f) Hand Vein, (g) Fingerprint, (h) Gait, (i) Hand Geometry, (j) Iris, (k) Palmprint, (l) Retina, (m) Signature
Source: Rishabh & Sandeep (2012)

### 2.1 Functional Properties of Biometric Traits

Certain factors are to be considered when assessing the suitability of any trait for use in biometric authentication. [7] identified some factors to include universality, uniqueness, measurability, performance, acceptability and circumvention.

However, [4] argued that the requirements of a biometric feature are uniqueness, universality, permanence, measurability, user friendliness, collectible and acceptability.

(*i*) *universality* means that every person should have the characteristic,

(*ii*) *uniqueness* indicates that no two persons should be the same in terms of the characteristic,

(*iii*) *permanence* means that the characteristic should be invariant with time and environment

(*iv*) *collectability* indicates that the characteristic can be measured quantitatively.

In practice, there are some other important requirements:

*(i)* *performance*, which refers to the achievable identification accuracy, the resource requirements to achieve an acceptable identification accuracy, and the working or environmental factors that affect the identification accuracy,

*(ii)* *acceptability*, which indicates to what extent people are willing to accept the biometric system, and

*(iii)* *circumvention*, which refers to how easy it is to fool the system by fraudulent techniques.

### 2.2 Components of all Biometric Systems

A modern biometric system consists of six modules: sensors, aliveness detection, quality checker, feature-generator, matcher and decision modules [14].

Sensors, which are the most important part of a ‘biometric capture device’, target physical properties of body parts, or physiological and behavioral processes, which are called ‘biometric characteristics’. The output of the sensor(s) is an analogical, or digital, representation of the biometric characteristic, this representation is called a ‘biometric sample’.

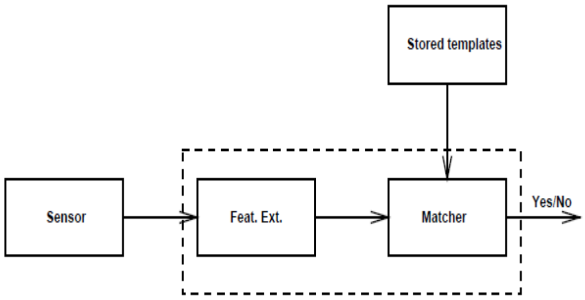

Fig 2: A Generic Biometrics System
Source: Nalini et al (2000)

## 3. The Human Body Odor

Every human body exudes an odor that characterizes its chemical composition and which could be used for distinguishing various individuals [9]. That means, body odor is one of the physical characteristics of a human that can be used to identify people. The human odor is released from various parts of body and exists in various forms such as exhalation, armpits, urine, stools, farts or feet [3].

The study of odors is a growing field but is a complex and difficult one. The complexity of odors arises from the sensory nature of smell [3]. The perception of odor sensation is hard to investigate because exposure to a volatile chemical elicits a different response based on sensory and physiological signals, and interpretation of these signals influenced by experience, expectations, personality or situational factors.

Odors are mixtures of light and small molecules that, coming in contact with various human sensory systems, also at very low concentrations in the inhaled air, are able to stimulate an anatomical response: the experienced perception is the odor [10].

Body odor serves several functions including communication, attracting mates, assertion of territorial rights, and protection from a predator [3]. A component of the odor emitted by a human body is distinctive to a particular individual. It is not clear if the invariance in a body odor could be detected despite deodorant smells, and varying chemical composition of the surrounding environment [9]. The odor biometric modality can been applied to many industrial applications including indoor air quality, health care, safety, security, environmental monitoring, quality control of beverage/food products and food processing, medical diagnosis, psychoanalysis, agriculture, pharmaceuticals, biomedicine, military applications, aerospace, detection of hazardous gases and chemical warfare agents [10].

### 3.1 Human Body Odor Acquisition Analysis

The human odor is released from various parts of body and exists in various forms such as exhalation, armpits, urine, stools, farts or feet [3]. Each chemical of the human odor is extracted by the biometric system and converted into a unique data string. The quality checker module performs a quality check on biometric samples and indicates whether the characteristic should be sensed again. Also, the quality check module may become responsible for producing extra data if the system is set for accepting only high resolution samples.

The most important element of a quality metric is its utility. Biometric samples with the highest resolution do not necessarily result in a better identification, while they always result in being redundant [16]. The feature-generator module extracts discriminatory features from biometric samples and generates a digital string called ‘biometric features’. A whole set of these features then constitute the ‘biometric template’.

Templates could be used to recreate artifacts that might be exploited for spoofing the system; such a possibility should be prevented by using encrypted templates. It is important that compressed biometric samples are not stored in the system or included in the template together with template encryption as this measure is vital to avoid the main risks of template misuse (e.g. identity theft, data mining and profiling) [16].

The matcher module compares the template with one or more templates previously stored. The decision module takes the final decision about personal identity according to the system’s threshold for acceptable matching. Extra data can hardly be generated by these two modules; their ethical and privacy relevance chiefly concerns the setting of the threshold for acceptable matching, which is not a trivial fact because it determines false rejections and false acceptance rates [16].

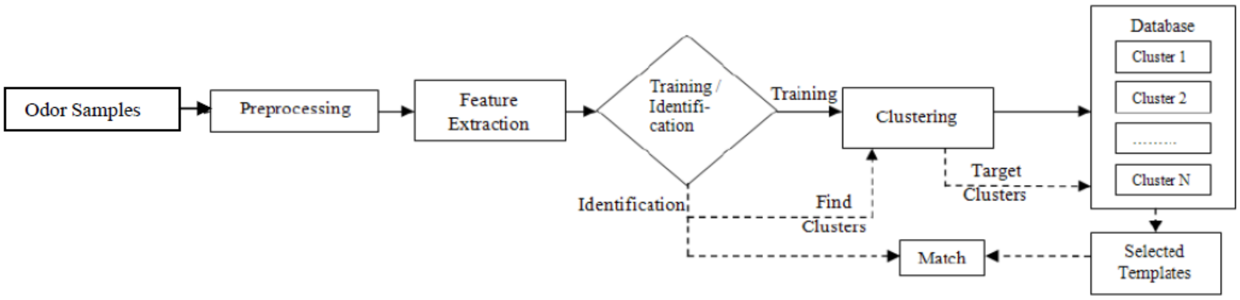

Fig 3: A Typical Odor Biometric Identification System
Source: Natale et al (2000)

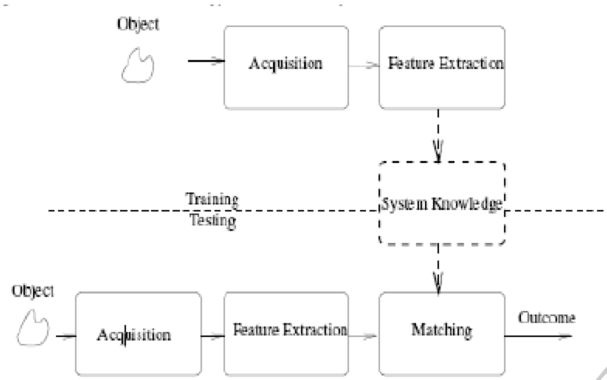

Fig 4: Odor Biometric Training and Testing System for identification
Source: Natale et al (2000)

### 3.2 Odor Detection and Classification

Despite the importance of perception of odor and flavor, there are problems in comparing different persons‘experience of smell and in quantifying odor. This need has created a need for a more analytical approach to the quantitative measurement of odor. For this purpose, the field of instrumental analyzers such as Electronic Noses (E-Noses) and Olfaction Systems (Machine Olfaction) has been developed in response to this need [13].

### 3.2.1 Electronic Noses (E-Noses)

Electronic/artificial noses are being developed as a system for the automated detection and classification of odors, vapors and gases. E-Nose is represented as a combination of two components: sensing system and pattern recognition system.

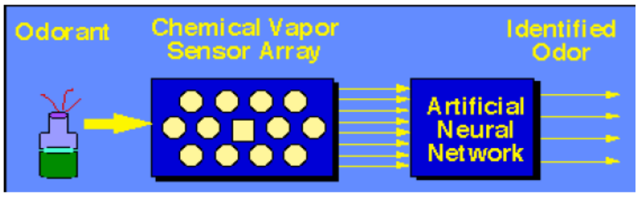

Fig 5: Schematic Diagram of E-Nose
Source: Zhanna (2005)

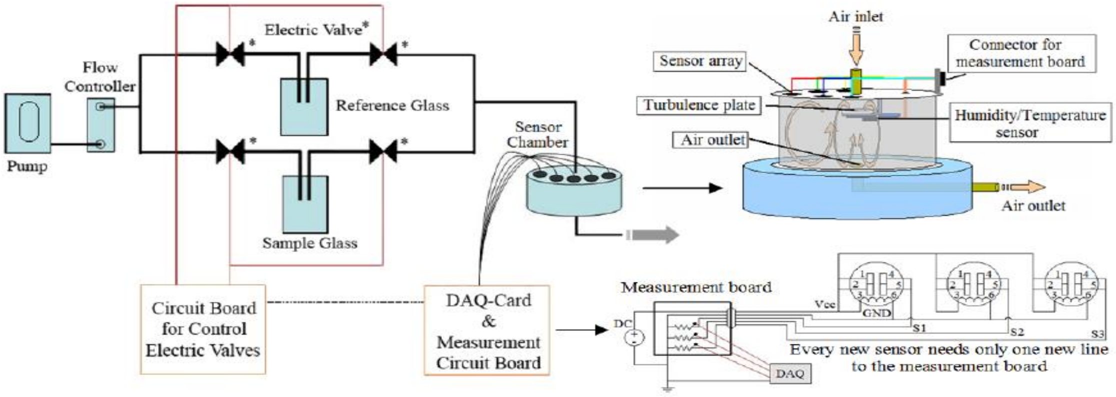
Electric Valve*
Flow Controller
Reference Glass
Pump
Sensor Chamber
Sample Glass
Circuit Board for Control Electric Valves
DAQ-Card & Measurement Circuit Board
Air inlet
Sensor array
Connector for measurement board
Turbulence plate
Humidity/Temperature sensor
Air outlet
Air outlet
Measurement board
Vcc
GND
DC
S1
S2
S3
DAQ
Every new sensor needs only one new line to the measurement board

Fig 6: Schematic diagram of the lab-made E-nose system
Source: Chatchawal et al (2009)

### 3.2.1.1 Sensing System

Sensing system allows tracing the odor from the environment. This system can be single sensing device, like gas chromatograph and spectrometer. In this case it produces an array of measurements for each component. The second type of sensing system is an array of chemical sensors. It is more appropriate for complicative mixtures because each sensor measure a different property of the sensed chemical [13]. Hybrid of single sensing device and array of chemical sensors is also possible. Each odorant presented to the sensing system produces a characteristic pattern of the odorant. By presenting a mass of sundry odorants to this system a database of patterns is built up and used to construct the odor recognition system.

### 3.2.1.2 Pattern Recognition System

Pattern recognition system is the second component of electronic nose used for odor recognition. Its goal is to train or to build the recognition system to produce unique classification or clustering of each odorant through the automated identification [3]. Unlike human systems, electronic noses are trained to identify only a few different odors or volatile compounds. There is a very strong restriction to use these noses for human recognition. State-of-the-art approaches do not make it possible to identify all components of the human body precisely. As such, recognition process incorporates several approaches: Statistical, ANN and Neuromorphic.

Many of the *statistical* techniques are complementary to ANNs and are often combined with them to produce classifiers and clusters. It includes PCA, partial least squares, discriminant and cluster analysis [16]. PCA breaks apart data into linear combinations of orthogonal vectors based on axes that maximize variance. To reduce the amount of data, only the axes with large variances are kept in the representation [17]. When an *ANN* is combined with the sensor array, the number of detectable chemicals is generally greater than the number of unique sensor types. A supervised approach involves training a pattern classifier to relate sensor values to specific odor labels. An unsupervised algorithm does not require predetermined odor classes for training. It essentially performs clustering of the data into similar groups based on the measured attributes or features [17].

### 3.2.2 Olfactory Signal Processing

The goal of an electronic nose is to identify an odorant sample and to estimate its concentration in human recognition case. It means signal processing and pattern recognition system. However, those two steps may be subdivided into preprocessing, feature extraction, classification and decision-making [13]. But first, a database of expected odorants must be compiled, and the sample must be presented to the nose’s sensor array.

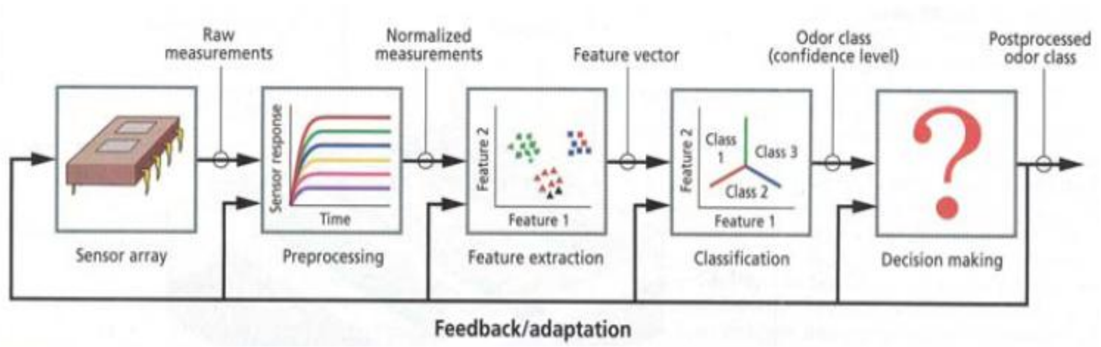

Fig 7: Signal Processing and Pattern Recognition systems stages
Source: Zhanna (2005)

The signal processing and pattern recognition are explicitly discussed below [13]:

*A. Preprocessing*

Preprocessing compensates for sensor drift, compresses the response of the sensor array and reduces sample-to-sample variations. Typical techniques include: normalization of sensor response ranges for all the sensors in an array; and compression of sensor transients.

*B. Feature extraction*

Feature extraction has two purposes: to reduce the dimensionality of the measurement space, and to extract information relevant for pattern recognition. Feature extraction is generally performed with linear transformations such as the classical PCA.

*C. Classification*

The commonly used method for performing the classification task is artificial neural networks (ANNs). An artificial neural network is an information processing system that has certain performance characteristics in common with biological neural networks. It allows the electronic nose to function in the way similar to brain function when it interprets responses from olfactory sensors in the human nose.

*D. Decision Making*

The classifier produces an estimate of the class for an unknown sample along with an estimate of the confidence placed on the class assignment. A final decision-making stage may be used if any application-specific knowledge is available, such as confidence thresholds or risk associated with different classification errors. The decision-making module may modify the classifier assignment and even determine that the unknown sample does not belong to any of the odorants in the database.

### 3.3 Odor Quantitative Analysis Metrics

Different aspects of odor can be measured through a number of quantitative methods including concentration and apparent intensity assessment.

### 3.3.1 Odor Concentration

An olfactometer test is used to measure odor concentration, which employs a panel of human noses as sensors [12]. In the olfactometry testing procedure, a diluted odorous mixture and an odor-free gas are presented separately from sniffing ports to a group of e-noses, kept in an odor-neutral room. The gases emitted from each sniffing port are compared, after which the presence of odor is determined alongside the confidence level such as guessing, inkling, or certainty of their assessment. The gas-diluting ratio is then decreased by a factor of two (i.e. chemical concentration is increased by a factor of two). This process is repeated and continues for a number of dilution levels [12]. The responses of the e-noses over a range of dilution settings are used to calculate the concentration of the odor in terms of European Odor Units (ouE/m$^3$). The main panel calibration gas used is Butan-1-ol, which at a certain diluting gives 1 ouE/m$^3$ [12]. The concentration is expressed as the dilution required for achieving panel detection threshold. Mathematically, the concentration is expressed as [10].

$$C = \frac{V_0 + V_f}{V_0}$$

where C is the odour concentration, V0 the volume of odorous sample and Vf the volume of odour-free air required to reach the threshold.

By analogy, for a dynamic olfactometer the concentration is given by (Magda, 2011):

$$C = \frac{Q_0 + Q_f}{Q_0}$$

### 3.3.2 Odor Intensity

Odor intensity is the perceived strength of odor sensation. This intensity property is used to locate the source of odors and perhaps most directly related to odor nuisance [18]. Perceived strength of the odor sensation is measured in conjunction with odor concentration. This can be modeled by the Weber-Fechner law [11].

$I$ = a * log(c)+b where

*I* is the perceived psychological intensity at the dilution step on the butanol scale, *a* is the Weber-Fechner coefficient, *C* is the chemical concentrations and *b* is the intercept constant (0.5 by definition). Odor intensity can be expressed using an odor intensity scale, which is a verbal description of an odor sensation to which a numerical value is assigned (Jiang, 2006).

Odor intensity can be divided into the following categories according to intensity: 0 - no odor, 1 - very weak (odor threshold), 2 – weak, 3 – distinct, 4 – strong, 5 - very strong and 6 – intolerable

### 3.4 Odor Biometrics Performance Metrics

The following parameters are generally used to measure the efficiency of a biometric system (Henshaw et al, 2006):

### 3.4.1 False Acceptance Rate (FAR)

The FAR is the frequency that a non authorized person is accepted as authorized. Because a false acceptance can often lead to damages, FAR is generally a security relevant measure. FAR is a non-stationary statistical quantity which does not only show a personal correlation, it can even be determined for each individual biometric characteristic (called personal FAR).

Due to the statistical nature of the false acceptance rate, a large number of fraud attempts have to be undertaken to get statistical reliable results. The fraud trial can be successful or unsuccessful. The probability for success FAR(n) against a certain enrolled person n is measured:

$$FAR(n) \ = \frac{Number\ of\ successful\ independent\ fraud\ attempts\ against\ a\ person\ (or\ characteristic)n}{Number\ of\ all\ independent\ fraud\ attempts\ against\ a\ person\ (or\ characteristic)n}$$

These values are more reliable with more independent attempts per person/characteristic. In this context, independency means that all fraud attempts have to be performed with different persons or characteristics! The overall FAR for N participants is defined as the average of all FAR(n):

$$FAR = \frac{1}{N}\sum_{n=1}^{N} FAR(n)$$

The values are more accurate with higher numbers of different participants/characteristics (N). Usually, during FAR determination, a fraud attempt is an attack using the characteristics of non-authorized persons. This, however, presents a high security which may not be present since there are a lot of further possibilities for promising attacks. A fraud attempt is *successful* if the user interface of the application provides a "successful" message or if the desired access is granted. A fraud attempt counts as *rejected* if the user interface of the application provides an "unsuccessful" message. In cases where no "unsuccessful" message is available, a verification time interval has to be given to ensure comparability. If the verification time interval has expired the fraud attempt is counted *unsuccessful*.

### 3.4.2 False Rejection Rate (FRR)

The FRR is the frequency that an authorized person is rejected access. FRR is generally thought of as a comfort criteria, because a false rejection is most of all annoying. FRR is a non-stationary statistical quantity which does not only show a strong personal correlation, it can even be determined for each individual biometric characteristic (called personal FRR).

Due to the statistical nature of the false rejection rate, a large number of verification attempts have to be undertaken to get statistical reliable results. The verification can be successful or unsuccessful. In determining the FRR, only fingerprints from successfully enrolled users are considered.

The probability for lack of success (FRR(n)) for a certain person is measured:

$$FRR(n) = \frac{\text{Number of rejected verification attempts for a qualified person (or feature)}n}{\text{Number of all verification attempts for a qualified person (or feature)}n}$$

These values are better with more independent attempts per person/feature. The overall FRR for N participants is defined as the average of FRR(n):

$$FRR = \frac{1}{N}\sum_{n=1}^{N} FRR(n)$$

The values are more accurate with higher numbers of participants (N). The determined FRR includes both poor picture quality and other rejection reasons such as finger position, rotation, etc. in the reasons for rejection. In many systems, however, rejections due to bad quality are generally independent of the threshold.
A verification attempt is *successful* if the user interface of the application provides a "successful" message or if the desired access is granted. A verification attempt counts as *rejected* if the user interface of the application provides an "unsuccessful" message. In cases of no reaction, a verification time interval has to be given to ensure comparability. If the time interval has expired the verification attempt is counted *unsuccessful*.

### 3.4.3 Failure to Enrol rate (FTE, also FER)

The FER is the proportion of people who fail to be enrolled successfully. FER is a non-stationary statistical quantity which does not only show a strong personal correlation, but can even be determined for each individual biometric characteristic (called personal FER). Those who are enrolled yet but are mistakenly rejected after many verification/identification attempts count for the Failure to Acquire (FTA) rate. The FTA usually is considered within the FRR and need not be calculated separately.

### 3.4.4 False Identification Rate (FIR)

The False Identification Rate is the probability in an identification that the biometric features are falsely assigned to a reference. The exact definition depends on the assignment strategy; namely, after feature comparison, often more than one reference will exceed the decision threshold.

### 3.4.5 Relative Operating Characteristic (ROC)

In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In biometric systems, the FAR and FRR can typically be traded off against each other by changing those parameters. The ROC plot is obtained by graphing the values of FAR and FRR, changing the variables implicitly.

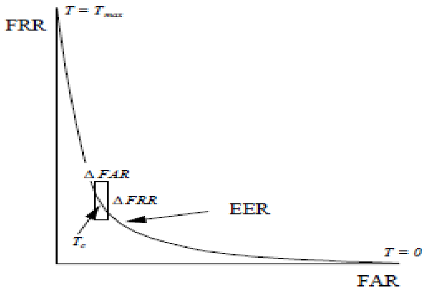

Fig 8: Receiver Operating Curve (ROC)
Source: Nalini et al (2000)

### 3.4.6 Equal Error Rate (EER)

This is the rate at which both accept and reject errors are equal. ROC plotting is used because how FAR and FRR can be changed, is shown clearly. When quick comparison of two systems is required, the EER is commonly used. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.

### 3.4.7 Failure to Capture Rate (FTC)

Within automatic systems, the probability that the system fails to detect a biometric characteristic when presented correctly is generally treated as FTC.

### 3.4.8 Template Capacity

It is defined as the maximum number of sets of data which can be input in to the system.

## 4 Conclusion

This study explicitly and theoretically analyzes odor biometric system for human recognition. It presents a comprehensive analysis of the technical, design and implementation issues relative to the application of odor biometric features for human recognition. The knowledge unveiled in this study will assist security system developers to understand the properties of odor biometric systems, its strengths and weaknesses as a unified biometric system or as a system to be multi-modally combined with other biometric modality (ies) to realize a more robust human recognition system.

## 5. References

[1] Duan, Xufang; Block, Eric; Li, Zhen; Connelly, Timothy; Zhang, Jian; Huang, Zhimin; Su, Xubo; Pan, Yi et al. (2012). "Crucial role of copper in detection of metal-coordinating odorants.". Proc. Natl.

Acad. Sci. U.S.A (109): Early Edition. doi:10.1073/pnas.1111297109.

[2] Olufemi Sunday Adeoye. (2010). "A Survey of Emerging Biometric Technologies". International Journal of Computer Applications, Volume 9– No.10, pg 1-5.

[3] Chatchawal Wongchoosuk, Mario Lutz and Teerakiat Kerdcharoen. (2009). "Detection and Classification of Human Body Odor Using an Electronic Nose". *Sensor. 9,* 7234-7249; doi:10.3390/s90907234

[4] Rishabh parashar, Sandeep Joshi. (2012). "Proportional Study of Human Recognition Methods". International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 6. Pg 47-51.

[5] Jain, A., Hong, L., & Pankanti, S. (2000). "Biometric Identification". *Communications of the ACM*, 43(2), p. 91-98. DOI 10.1145/328236.328110

[6] Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn, P; Ross, A. *Handbook of Biometrics*. Springer. pp. 1–22. ISBN 978-0-387-71040-2.

[7] Jain, A.K.; Bolle, R.; Pankanti, S., eds. (1999). *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publications. ISBN 978-0792383451.

[8] Wang, J.; Luthey-Schulten, Z.; Suslick, K. S. (2003). "Is the Olfactory Receptor A Metalloprotein?". *Proc. Natl. Acad. Sci. U.S.A.* (100): 3035–3039.

[9] Bhawani Radhika (2009). "Biometric Identification Systems": Feature Level Clustering of Large Biometric Data and DWT Based Hash Coded Ear Biometric System. An unpublished thesis submitted to the Department of Computer Science and Engineering, National Institute of Technology (Deemed University), Rourkela for the award of Bachelor of Science in Computer Science.

[10] Magda Brattoli, Gianluigi de Gennaro, Valentina de Pinto, Annamaria Demarinis Loiotile, Sara Lovascio and Michele Penza (2011). "Odour Detection Methods": Olfactometry and Chemical Sensors. Sensors 2011, 11, 5290-5322;

[11] Jiang, J., Coffey, P., & Toohey, B. (2006). Improvement of odor intensity measurement using dynamic olfactometry. Journal of the Air & Waste Management Association (1995), 56, 5, 675-83

[12] Feng, L.; Musto, C.J.; Suslick, K. S. (2010) "A Simple and Highly Sensitive Colorimetric Detection Method for Gaseous Formaldehyde". J. Am. Chem. Soc (132): 4046–4047.

[13] Zhanna Korotkaya (2005). "Biometric Person Authentication": Odor. Department of Information Technology, Laboratory of Applied Mathematics,Lappeenranta University of Technologypg 1-16

[14] Emilio Mordini and Sonia Massari (2008). "Body Biometrics and Identity". *Bioethics* ISSN 0269-9702 (print); 1467-8519 (online), *Volume 22 Number 9 2008* pp 488–498.

[15] Nalini K. Ratha, Andrew Senior and Ruud M. Bolle (2000). "Automated biometrics". IBM Thomas J. Watson Research Center, P. O. Box 218, Yorktown Heights, NY 10598, pg 1-11.

[16] Natale, C.D.; Macagnano, A.; Paolesse, R.; Tarizzo, E.; Mantini, A.; D'Amico, A. (**2000). "**Human Skin Odor Analysis by Means of an Electronic Nose". *Sens. Actuat. B*, 65, 216–219.

[17] Penn, D.J.; Oberzaucher, E.; Grammer, K.; Fischer, G.; Soini, H.A.; Wiesler, D.; Novotny, M.V.; Dixon, S.J.; Xu Y.; Brereton, R.G. (2007). "Individual and Gender Fingerprints in Human Body Odour". *J. R. Soc. Interf.*, *4*, 331–340.

[18] Spengler 2000, p.492. doi:10.3390/s110505290. www.mdpi.com/journal/sensors