International Research Journal of Computer Science (IRJCS)
Issue 09, Volume 5 (September 2018)
ISSN: 2393-9842
www.irjcs.com

OVERVIEW OF MULTIBIOMETRIC SYSTEMS

Adedeji O. T.,
Department of Computer Science and Engineering,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria
otadedeji@lautech.edu.ng
Falohun A.S.,
Department of Computer Science and Engineering,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria
asfalohun@lautech.edu.ng
Alade O. M.,
Department of Computer Science and Engineering,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria
oalade75@lautecg.edu.ng
Amusan E. A.,
Department of Computer Science and Engineering,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria
eaamusan@lautech.edu.ng

Manuscript History
Number: **IRJCS/RS/Vol.05/Issue09/SPCS10081**
Received: 10, September 2018
Final Correction: 21, September 2018
Final Accepted: 27, September 2018
Published: September 2018
Citation: Adedeji, Falohun, Alade & Amusan (2018). OVERVIEW OF MULTIBIOMETRIC SYSTEMS. IRJCS:: International Research Journal of Computer Science, Volume V, 459-466. **doi://10.26562/IRJCS.2018.SPCS10081**
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract-- User verification systems that use a single source of biometric information are not sufficient to meet today's high security requirements for applications. This is because these systems have to contend with noisy data, intra-class variations, spoof attack and non-universality. Therefore, there is need for employing multiple sources of biometric information to provide better recognition performance as compared to the systems based on single trait. This paper is an overview of different categories of multibiometric systems, information fusion in multibiometric systems, and approaches to feature fusion at feature selection phase.

Keywords: Biometrics; Multibiometric System; Fusion; Feature Extraction; Feature Selection;

I. INTRODUCTION

Biometric is the science and technology of measuring and analyzing biological data (Choudhary, 2012). In information technology, biometrics refers to technologies that measure and analyze human body characteristics (Jain and Ross, 2004; Omidiora, 2006; Omidiora *et. al.*, 2008). A biometric system is basically a pattern recognition system that recognizes a person based on a set of features derived from specific physiological or behavioural characteristics that the person possesses (Prabhakar, Pankanti and Jain, 2003). Biometric systems are advantageous because they do not require a person to carry cards or remember information unlike conventional authentication systems, which are either possession-based or knowledge-based (Omidiora, 2006; Kim, Shin, Lee and Park, 2012). These conventional methods are unreliable because keys and cards can be lost or stolen, likewise passwords can be compromised, forged or hacked (Omidiora, 2006; Falohun, 2012). Therefore, biometric system has been adopted in many applications (Kim *et. al.*, 2012). However, these systems still have to contend with a variety of problems such as noisy data, inter-class similarities, intra-class variations to mention a few.

It is therefore apparent that unibiometrics is not sufficient to achieve the desired performance in real world applications especially those that demands strong authentication (Sanjekar and Patil, 2013). This problem can be resolved using multibiometric system (Nahdeen and Poornima, 2013).

II. DESIRABLE PROPERTIES OF BIOMETRIC TRAIT

Physiological or behavioural trait should satisfy the following characteristics to be considered for biometric system (Jain and Ross, 2004; Omidiora, 2006: Falohun, 2012).

(i) Invariance / permanence: A good biometrics' intra-class variability must be relatively minimal over a long period of time. This would eliminate the need for constant updates to the database that stores the biometric templates.
(ii) Universality: A good biometric system should be possessed by all individuals.
(iii) Uniqueness: No two individual should have the same value of the biometric characteristics.
(iv) Measurability and Reducibility: A good biometric should be easy to measure and be transformed into digital or other mathematically tractable form for manipulation by computer.

III. ADVANTAGES OF BIOMETRIC SYSTEM

Biometric system offers many advantages over the traditional authentication methods, some of which are highlighted below (Omidiora, 2006; Mane and Jadhav,2009; Mishra, 2010; Falohun, Omidiora, Fakolujo, Afolabi, Oke and Ajala, 2012):

(i) Unlike passwords and tokens, biometric trait cannot be lost, forgotten and forged.
(ii) Biometric trait cannot be easily copied, shared, distributed or forged.
(iii) It adds to user convenience by alleviating the need to design and remember passwords.
(iv) Use of biometric can provide negative recognition and guarantee non-repudiation

IV. CLASSIFICATION OF BIOMETRIC SYSTEM

Various biometric traits can be grouped into two broad categories:

(i) Systems classified according to the type of traits used
(ii) Systems classified according to the number of biometric information used.

A. Biometric system classified according to the type of traits used.

The biometric systems are classified into three categories based on the nature of the trait used:

(i) Physiological features based biometric system
(ii) Behavioural features based biometric system
(iii) Chemical features based biometric system

(i) Physiological Features based Biometric System

This is biometric systems that make use of physiological characteristics of an individual for identification/verification purposes. A physiological feature is a feature that is physically present in the body of a person. These features are extracted from human body using specific equipment and techniques. Physiological biometric features include iris image, fingerprint, face, palmprint, DNA sequence. They are more stable and permanent in nature and not easy to imitate.

(ii) Behavioural features based biometric system

This category of biometric systems measures behavioural trait of an individual in order to identify the person. The behavioural features are the features which are extracted from day-to-day sociological behavior of a person. Behavioural biometric system measures the way in which a user performs certain tasks. They are usually temporal in nature and can be forged easily. The behavioural features based biometric systems have low accuracy, high FRR, and low FRR. Therefore, a single behavioural feature based biometric system will not be sufficient for identifying a person.

(iii) Chemical features based biometric system

This is not a popular biometrics and involves measurement of chemical cues such as order and the chemical composition of human perspiration.

B. Biometric system classified according to the number of biometric information used

Biometric systems are classified into two based on the number of information used in idenfication/verification (Bhawna, Simerpreet and Sunita, 2012):

(i) Unibiometric System
(ii) Multibiometric System

(i) Unibiometric system

This kind of biometric system employs the use of one biometric information for identification purposes. The information may be obtained from physiological, behavioural or chemical trait of an individual. This is popularly known as Unimodal biometric system.

Despite considerable advances in recent years, there are still serious challenges in obtaining reliable authentication through unibiometric system. This is because each trait has its own limitations, therefore unibiometric systems are limited in performance and are not sufficient for full proof identification of a person (Jain and Ross, 2004; Bhawna, *et. al.,* 2012).

V. LIMITATIONS OF UNIMODAL BIOMETRIC SYSTEM

The following are the observed limitations of unibiometric systems that are already in use (Jain and Ross, 2004; Jain *et. al.*, 2004; Kaur and Sharma, 2013):

(a) Noise in sensed data: The biometric captured may be noisy or distorted due to defective or improper maintained devices, or scar. Noisy data can also result from accumulation of dirt on a sensor or from ambient conditions. This leads to higher error rates in biometric system.

(b) Intra-class variations: Biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment. The variation may be due to improper interaction of the user with the sensor, use of different sensors during enrollment and verification, changes in the ambient environmental conditions and inherent changes in the biometric trait.

(c) Distinctiveness: While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This restricts the discriminability provided by the biometric trait.

(d) Non-universality: Non-universality means the possibility that a subset of users do not possess the biometric trait being acquired. While it is expected that every user should possess the biometric trait being acquired, in reality it is possible that a group of users do not possess that particular biometric characteristics.

(e) Spoof attacks: Biometric spoofing means that it is possible for unimodal systems to be fooled. For instance, an individual may attempt to fool an iris recognition system through the use of contact lenses with copied patterns.

(ii) Multibiometric system

According to the International Committee for Information Technology Standard (INCITS), multibiometric system indicates the presence and use of more than one biometric aspect (modality, sensor, instance and/ or algorithm) in some form of combined use for making a specific biometric verification / identification (Mishra, 2010; Shreya and Ephin, 2013).

VI. MULTIBIOMETRIC SYSTEM

Some of the limitations of unimodal biometric system can be overcome by including multiple sources of information for establishing the identity of a person (Jain and Ross, 2004; Kaur and Sharma, 2013). The goal of multibiometric system is to reduce one or more of the following:

(i) False Accept Rate (FAR)
(ii) False Reject Rate (FRR)
(iii) Failure to Enroll (FTE)
(iv) Susceptibility to artifacts or mimicks.

VII. CATEGORIES OF MULTI-BIOMETRIC SYSTEMS

Based on the sources of information, the following six categories of multibiometric systems have been identified (Mane and Jadhav, 2009; Bhawna *et. al.,* 2012)

(i) **Multiple sensors - one biometric trait:** In these systems, different sensors are used for capturing different representations of the same biometric modality to extract different information. For example, a biometric system may use 2D, 3D or X-ray images for authentication. As these systems consider only one biometric trait, so, if the biometric system is not appropriate, one can't get any benefit from the multiple acquisition of the biometric trait.

(ii) **Multiple instances** - one biometric trait: In these systems, multiple instances of the same biometric trait are used for authentication.

For example, the image of left and right eye of a subject may be used for retina recognition system. These systems are cost efficient, as the same sensors or the same feature extraction and matching algorithm can be used.

(iii) **Multiple algorithms** - one biometric trait: These systems use one biometric trait but use different matching algorithms. For example, a system may use eigenface and Voronoi diagram as matching algorithms for the same set of face images and later combine the results. These systems also suffer with the poor quality of input.

(iv) **Multiple samples with single sensor - one biometric trait**: These systems use single sensor but multiple samples of the same biometric trait. For example, a single sensor may be used to capture different facial expression images of a subject and latter a mosaicing scheme may be used to build a composite face image from all the available face images of that subject.

(v) **Multimodal system**: These systems use more than one biometric traits and hence are referred to as multimodal systems. For example, a biometric system may use face and voice for person authentication. The cost of deploying these systems is substantially more due to the requirements of new sensors and for the development of the new user interface.

(vi) **Hybrid systems**: These systems use more than one scenarios discussed above for robust authentication. For example, a biometric system may use two iris matching algorithms and three face matching algorithms in one face and iris based multimodal biometric system.

VIII. INFORMATION FUSION IN MULTIBIOMETRIC SYSTEMS

Biometric fusion is the term used to describe the mechanism for integrating data from two or more traits. It refers to the consolidating of information or evidences presented by multiple biometric sources (Ross and Jain, 2003; Shanthini and Swamynathan, 2012). Based on this, Sanderson and Paliwal (2002) classified information fusion into pre-mapping fusion, midst-mapping fusion and post-mapping fusion. In pre-mapping fusion, information is combined before the use of classifier or expert; in midst-mapping fusion, information is combined during mapping from sensor/feature space into opinion/decision space, while in post-mapping fusion, information is combined after mapping from sensor/feature space into opinion/decision space. Pre-mapping fusion is categorized into sensor level fusion and feature level fusion. In post-mapping fusion, there are two main categories: decision level fusion and score level fusion.

(a) Pre-mapping fusion I: Sensor level fusion: fusion at this level combines raw data acquired from sensing the same or different biometric traits with two or more sensors. There are two methods to combine data at sensor level: weighted summation and mosaic construction.

Weighted summation can be employed to combine visual and infrared images into one image, or, to combine data from two microphones. Mosaic construction can be employed to create one image out of images provided by several cameras, where each camera is observing a different part of the same object. Although fusion at such a level is expected to enhance the biometric recognition accuracy, it is not suitable for multimodal biometrics because of the incompatibility of data from different modalities (Sanderson and Paliwal, 2004).

(b) Pre-mapping fusion II: Feature level fusion: Fusion at this level can be applied to features extracted from the same modality or different modalities. Feature level fusion schemes can be categorized into two broad classes, namely homogeneous and heterogeneous. A homogeneous feature fusion scheme is used when the feature sets to be combined are obtained by applying the same feature extraction algorithm to multiple samples of the same biometric trait. This approach is applicable to multi-sample and multi-sensor systems.

Feature level fusion is expected to perform better than fusion at score level and decision level since feature set contains richer information about the raw biometric data (Delac and Grgic, 2004; Sanderson and Paliwal, 2004). Feature level fusion also increases the reliability of the system by preventing the biometric template from modification, and reduces the response time than score level fusion (Nahdeen and Poornima, 2013). However, feature level fusion is not widely adapted because of incompatibility between different feature vectors and high dimension of the resulting composite feature vector.

(c) Midst-mapping fusion: This is a relatively new and a more complex concept. Here, several information streams are processed concurrently while mapping from feature space into opinion/decision space. Midst-mapping fusion concept can be used for exploitation of temporal synergies between the streams. Furthermore, streams weights can be utilized in midst-mapping fusion to account for the reliability of different streams of information. Example of this type of fusion is extended Hidden Markov Models which have been shown useful for text-dependent person verification.

(d) Post-mapping fusion I: score level fusion: In this type of fusion, rather than combining the feature vectors, they are processed separately and individual matching score is found (Jain and Ross, 2004). Unlike decision fusion, in score-level fusion methods the experts do not provide final decisions but only opinions on each possible decision. In the case that matching score from the modalities are heterogeneous, score normalization is needed to transform these scores into common domain prior to combination (Jain and Ross, 2004). This is accomplished by mapping the output to the [0, 1] interval, where 0 indicates the lowest opinion and 1 the highest opinion.

The normalization techniques that are usually used are: min-max, decimal scaling, z-score, median and Median Absolute Deviation (MAD), double sigmoid, tanh-estimators and biweight estimators (Jain and Ross, 2004). Opinions can be combined using weighted summation or weighted product approaches before using a classification criteria such as the MAX operator which selects the class with the highest opinion to reach a decision. The natural benefit of weighted summation and product over feature vector concatenation and decision fusion is that the opinions from each expert can be weighted. The weight can be set to reflect the reliability and discriminability of each expert. Score-level fusion is very popular due to the easy access of information to be fused and easy implementation. However, the information obtained for fusion at the score level is limited compared to feature level fusion and may result in inferior performance. This is due to loss of information when fusion is conducted at higher levels (Jain and Ross, 2004).

(e) Post-mapping fusion II: Decision level fusion: Each modality is first pre-classified independently, and then final classification is based on the fusion of the output of the different classifiers. The classifiers can be of the same type but working on different features for instance audio and video data, non-homogeneous classifiers working with the same features, or a hybrid of the two types.

The decisions can be combined by majority voting, combination of ranked lists, or using AND / OR operators. The main disadvantage of this kind of fusion is that it seriously limits the basis for enhancing the system accuracy through the fusion process. Therefore, fusion at this level is the least powerful.

IX. METHODS FOR FEATURE LEVEL FUSION

Feature level fusion refers to combining different feature vectors that are obtained by either using multiple sensors or employing multiple feature extraction algorithms on the same sensor data (Dapinder and Gaganpreet, 2013). Feature level fusion can be done either at feature extraction stage or at feature selection stage (Awang *et. al.*, 2013; Adedeji *et. al.*,2015). Fusion at feature extraction stage can be achieved either by weighted summation method or by feature concatenation while that of feature selection stage is achievable by the use of nature inspired algorithms.

(a) Weighted summation: This method is used to combine homogeneous feature vectors at feature extraction level. This is achieved by calculating a single resultant feature vector. This method can be used to fuse multiple fingerprint impressions of a user's finger.

(b) Feature concatenation: When feature vectors are non-homogeneous, for instance, feature vectors obtained using different feature extraction techniques, or feature vectors of different biometric modalities; concatenation method can then be used to fuse them into a single feature vector. Concatenation is not possible when the feature sets are incompatible, for example, fingerprint minutiae and eigen face coefficients. It is only possible if the modalities have the same domain such as image based or signal based. However, in using two different modalities, methods of normalizing the different domain features are necessary in order to concatenate the features. This normalization technique used in score level fusion can also be applied for feature level fusion (Rattani, Kisku, Bicego and Tistarelli, 2007; Awang *et. al.,* 2013).

There are some downsides to the feature vector concatenation approach as stated by Sanderson and Paliwal (2004):

i. There is no explicit control over how much each vector contributes to the final decision.

ii. The separate feature vectors must be available at the same frame rate that is the feature extraction must be synchronous, which is a problem when combining speech and visual feature vectors.

1. The dimensionality of the resulting feature vector, which can lead to the 'curse of dimensionality' problem and the difficulty of finding a good classifier for the resulting high dimensional feature vectors (Aly *et. al.*, 2012).
2. Resulting high dimension feature vector increases computational and storage resources demand of the overall biometric system.

X. FUSION AT FEATURE SELECTION PHASE

In general, feature level fusion can be performed at feature extraction phase or feature selection phase (Awang *et. al.*, 2013). Most of feature level fusion is implemented at feature extraction phase. The goal of fusion at the feature selection phase is to combine the biometric traits and at the same time reduce the dimension of the feature vector. Feature selection can be defined as a process that chooses a minimum subset of *M* features from the original set of *N* features, so that the feature space is optimally reduced according to a certain evaluation criterion. The aim of feature selection is to fuse and reduce the features dimension prior the classification phase (Awang *et. al.*, 2013). The new feature vector from the feature selection will be in low dimension and consists of the features of all biometrics.

XI. APPROACHES TO FEATURE SELECTION PHASE FUSION

Feature selection is implemented to fuse the features as well as to select the best number of significant features.

The idea of feature selection in fusion is to select the most significant features from the modalities while maintaining balance between the selected features in order to meet the objective of the parallel multimodal biometrics system. Feature selection is a form of optimization problem in which the task is to find best features (minimum) that maximizes the performance of the biometric system. Numerous conventional optimization schemes have been proposed, developed and successfully implemented in literature. However, these schemes face difficulties in meeting the growing needs of modern industry, in which the existing optimization problems tend to be dynamic, constrained, multi-variable, multi-modal and multi-objective. Furthermore, most of the conventional optimization approaches are not efficient enough in dealing with practical large-scale systems (Wang, Han, Niu and Busch, 2009). Conventional optimization methods are limited by a weak global search ability, instability, and inefficiency, especially when attempting highly nonlinear optimization tasks. While nature inspired optimization algorithms have been shown to be more efficient for discontinuous, non-differentiable, multimodal, noisy problems (Wang *et. al.*, 2009). Nature inspired optimization algorithm is an emerging computing paradigm that draw their inspiration from diverse natural sources, including the operation of biological neurons, evolution process, and natural immune responses (Timmis, Andrews, Owens and Clark, 2008). These algorithms include Ant Colony Optimization (ACO), Particle Swarm Optimization (PSO), Genetic Algorithm (GA), Clonal Selection Algorithm (CSA).

A. Ant colony optimization (ACO) algorithm

The ACO metaheuristic was inspired by the foraging behavior of real ants. An ant colony system involves simple agents (ants) that cooperate with one another to achieve an emergent, unified behavior for the system as a whole, producing a robust system capable of finding high-quality solutions for problems with a large search space. In the context of rule discovery, an Ant Colony system has the ability to perform a flexible, robust search for a good combination of logical conditions involving values of the predictor attributes. ACO algorithm is characterized as being a distributed, stochastic search method based on the indirect communication of a colony of ants, mediated by pheromone trails. The pheromone trails in ACO serve as distributed numerical information used by the ants to probabilistically construct solutions to the problem under consideration. The ants modify the pheromone trails during the algorithm's execution to reflect their search experience (Dorigo and Stutzle, 2010).

In general, the ACO approach attempts to solve an optimization problem by repeating the following two steps:

(i) Candidate solutions are constructed using a pheromone model, that is, a parameterized probability distribution over the solution space;

(ii) The candidate solutions are used to modify the pheromone values in a way that is deemed to bias future sampling toward high quality solutions.

B. Particle swarm optimization (PSO) algorithm

The Particle Swarm Optimization (PSO) algorithm is a robust stochastic optimization technique based on the movement and intelligence of swarms (Huang and Wang, 2006; Krishneswari and Arumugam, 2012b). It is a multi-agent parallel search technique which maintains a swarm of particles and each particle represents a potential solution in the swarm. It was proposed by Eberhart and Kennedy in 1995 and has since then been used as a robust method to solve optimization problem in a wide variety of applications. It uses a number of agents (particles) moving around in the search space looking for the best solution (Krishneswari and Arumugam, 2012b). All particles fly through a multidimensional search space where each particle is adjusting its position according to its own experience and that of neighbours (Li and Deb, 2010). Therefore, the PSO algorithm is a member of swarm intelligence. In a PSO method, all particles are initiated randomly and evaluated to compute fitness together with finding the personal best (best value of each particle) and global best (best value of particle in the entire swarm). After that a loop starts to find an optimium solution. In the loop, first, the particles' velocity is updated by the personal and global bests, and then each particle's position is updated by the current velocity. The loop is ended with a stopping criterion predetermined in advance. PSO method was adapted by Krishneswari and Arumugam (2012b) for intra-modal feature level fusion.

C. Genetic algorithm (GA)

Genetic algorithm (GA) belongs to a group of methods, called evolutionary algorithms. It is a general adaptive optimization search methodology based on a direct analogy to Darwinian natural selection and genetics in biological systems, is a promising alternative to conventional optimization methods. In general, GA start with an initial set of random solutions called population. A GA basically has four components: A population of individuals where each individual in the population represents a possible solution; a fitness function which is an evaluation function by which an individual is accessed as good or bad. Awang et.al. (2013) modified GA for feature selection phase fusion of face and signature. Comparison of the performance of the proposed method with other approaches indicates the highest recognition accuracy of 97.50%.

D. Clonal Selection Algorithm (CSA)

Clonal Selection Algorithm (CSA) is a special class of Artificial Immune System inspired from the clonal selection principle of AIS. Clonal selection in AIS is the selection of a set of artificial lymphocytes (ALCs) with the highest affinity with non-self pattern (De Castro and Von Zuben, 2002; Cisar, Cisar and Markoski, 2014). Clonal selection principle describes how the immune cells eliminate a foreign antigen and is simple but efficient approximation algorithm for achieving optimum solution. CSA shares many similarities with GA but instead of crossover operator, it uses cloning operator to construct new generation of candidate solutions. A modified CSA was proposed by Adedeji *et. al.,*2015 for feature Level fusion of multibiometric systems.

XII. CONCLUSION

Biometric recognition refers to the automatic identification of a person based on his/her anatomical, behavioural or chemical characteristics. Biometric authentication is advantageous over traditional methods in that it cannot be stolen, forged or forgotten. However, these systems still have to contend with a variety of problems such as noisy data, inter-class similarities, intra-class variations to mention a few. It is therefore apparent that unibiometrics is not sufficient to achieve the desired performance in real world applications especially those that demands strong authentication. This problem can be resolved using multibiometric system. Feature level fusion at the feature selection phase is still not popular, future works can be tailored towards multimodal fusion at feature selection phase.

REFERENCES

[1]. Adedeji O. T, Omidiora, E. O., Olabiyisi, O. S., & Adigun, A. A. (2012). Performance Evaluation of Optimised PCA and Projection Combined PCA methods in Facial Images. *Journal of Computations & Modelling, 2*(3), 17-29.

[2]. Adedeji O. T, Falohun A. S, Alade O. M, Omidiora E. O. and Olabiyisi S. O. (2015): Development of a Modified Clonal Selection Algorithm for Feature Level Fusion of Multibiometric System, LAUTECH Journal of Engineering and Technology, 9(2):80-85.

[3]. Awang S., Yusof R., Zamzuri M. F. and Arfa R. (2013): "Feature Level Fusion of Face and Signature using a Modified Feature Selection Technique", International Conference on Signal-Image Technology and Internet-Based Systems, (IEEE-Computer Society): 706-713.

[4]. Bhawna K., Simerpreet K. and Sunita S. (2012): "Biometric Recognition Systems – Multimodal over Unimodal", International Journal of Engineering and Innovative Technology (IJEIT), 2(1):112-120.

[5]. Dapinder K. and Gaganpreet K. (2013): "Level of fusion in Multimodal Biometrics: a Review", International journal of Advanced Research in Computer Science and Software Engineering, 3(2): 242-246.

[6]. De Castro L. N. and Von Zuben F. J. (2002): "Learning and Optimization using the Clonal Selection Principle", IEEE Transaction on Evolutionary Computation, 6(3):239-251.

[7]. Delac K. and Gurgic M. (2004): "A survey of Biometric Recognition Methods", 46th International symposium of Electronics in marine, ELMAR-2004 Zadar Croatia.

[8]. Dorigo, M. and Stützle, T. (2010). Ant colony optimization: overview and recent advances *Handbook of metaheuristics* (pp. 227-263): Springer.

[9]. Falohun, A. (2012). Development of a Feature Extraction Method for Iris Recognition using Enhanced Inverse Analytical Fourier-Mellin Transform. *Unpublished Ph. D. Thesis*. Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

[10]. Falohun, A., Omidiora, E., Fakolujo, A., Afolabi, O., Oke, A., & Ajala, F. (2012). Development of a biometrically-controlled door system (using iris), with power backup. *AJSIR, 3*(4), 203-207.

[11]. Huang, C.-L. and Wang, C.-J. (2006). A GA-based feature selection and parameters optimizationfor support vector machines. *Expert Systems with applications, 31*(2), 231-240.

[12]. Jain A. K and Ross A. (2004): "Multibiometric systems", Communications of the ACM, Special issue on Multimodal Interfaces, 47(1):34-40.

[13]. Kaur S. and Sharma P. (2013): "Analysis of Multimodal Biometrics by Feature Level Fusion: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, 3(7): 1383-1392.

[14]. Kim Y. G., Shin K. Y., Lee E. C. and Park K. R., (2012): "Multimodal Biometric Sytem based on the Recognition of faces and Both Irises", International Journal of Advanced Robotic Systems, 9(65):1-6.

[15]. Krishneswari K. and Arumugam S (2012a): "Multimodal Biometrics Using Feature Fusion", Journal of Computer Science, 8(3): 431-435.

[16]. Krishneswari, K. and Arumugam, S. (2012b). Intramodal feature fusion based on PSO for palmprint authentication. *Int Journal on Image and Video Proc, 2*(4), 435-440.

[17]. Li, X., and Deb, K. (2010). *Comparing lbest PSO niching algorithms using different position update rules.* IEEE congress on evolutionary computation.

[18]. Mane, M. and Jadhav, D (2009): "Review of multimodal Biometrics: applications, challenges and research areas", International Journal of Biometrics and Bioinformatics (IJBB), 3(5): 90-95.

[19]. Mishra A. (2010): "Multimodal Biometrics it is: Need for future systems", International journal of Computer Application, 3(4): 28-33.

[20]. Nahdeen F. M. and Poornima S. (2013): "Feature Level Fusion in Multimodal Biometric Authentication System", International Journal of Computer Applications, 69(18): 36 – 40.

[21]. Omidiora E. O. (2006): "A Prototype of Knowledge-based System for Black Face Recognition System using Principal Component Analysis and Fisher Discriminant Algorithms", Unpublished Ph. D. Thesis, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

[22]. Omidiora, E., Fakolujo, O., Ayeni, R., Olabiyisi, S., & Arulogun, O. (2008). Quantitative evaluation of principal component analysis and fisher discriminant analysis techniques in face images. *Journal of Computer and its Applications, 15*(1), 22-37.

[23]. Prabhakar S., Pankanti S. and Jain A. K. (2003): "Biometric Recognition Security and Privacy concerns" IEEE Security & Privacy, :33-42.

[24]. Rattani A., Kisku D. R., Bicego M and Tistarelli M. (2007): "Feature Level Fusion of Face and Fingerprint Biometrics", First IEEE International Conference on Biometrics: theory, Applications and Systems.

[25]. Ross A. and Jain A. K. (2003): "Information Fusion in Biometrics", Pattern Recognition Letters, 24(13): 2115-2125.

[26]. Ross A. and Jain A. K. (2004): "Multimodal Biometrics: An Overview", Appeared in Proceedings of 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), :1221-1224.

[27]. Sanderson, C., and Paliwal, K. K. (2004). Identity verification using speech and face information. *Digital Signal Processing, 14*(5), 449-480.

[28]. Sanjeka, P.S. and Patil, J.B. (2013); "An overview of multimodal Biometrics", Signal and Image Processing: An International Journal (SIPIJ), 4(1):57-64.

[29]. Shanthini B. and Swamynathan S. (2012): "A Novel Multimodal Biometric Fusion Technique for Security", International Conference on Information and Knowledge management. 45(1):143-147.

[30]. Sharma, P. and Wadhwa, A. (2014). Analysis of Selection Schemes for Solving an Optimization Problem in Genetic Algorithm. *International Journal of Computer Applications, 93*(11).

[31]. Shreya Mohan and Ephin M (2013): "Advanced Authentication Scheme using Multimodal Biometric Scheme", International Journal of Computer Applications Technology and Research 2(2):170 – 175.

[32]. Timmis, J., Andrews, P., Owens, N. and Clark, E. (2008). An interdisciplinary perspective on artificial immune systems. *Evolutionary Intelligence, 1*(1), 5-26.

[33]. Wang Z., Han Q., Niu X. and Busch C. (2009): "Feature Level Fusion of Iris and Face for Personal identification", Proceeding of the 6th international Symposium on Neural Networks, 356-364.

