ISSN 2319 – 7757 EISSN 2319 – 7765

Indian Journal of Engineering

Role of multibiometric systems in analysis of biological data

Karpagavalli K[1]☼, Ramakrishnan S[2]

1. Department of Physics, SRR Engineering College, Padur, Chennai, Tamil Nadu, India
2. Department of Information Technology, Velammal Engineering College, Tamil Nadu, India

☼***Corresponding author:*** Research Scholar, Department of Computer Science, Sathyabama University, Tamilnadu, India, Mail: karpagasri@rediffmail.com, ramkrishod@gmail.com

Received 04 May; accepted 12 June; published online 01 July; printed 16 July 2013

ABSTRACT

Biometric authentication refers to technologies that measure and analyzes human physical and behavioral characteristics for authentication purposes. Examples of physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while examples of mostly behavioral characteristics include signature, gait and typing patterns. Voice is considered a mix of both physical and behavioral characteristics. However, it can be argued that all biometric traits share physical and behavioral aspects. This paper deals with Multibiometric applications in biological data analysis. It outlines the sources of multiple evidence, multi algorithm systems, multi instance systems, multi sample systems and multimodal systems. This paper concludes with some interesting findings.

Key words: biometric, biological data, multimodal systems

1. INTRODUCTION

The terms “Biometrics” and “Biometry” have been used since early in the 20th century to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. Statistical methods for the analysis of data from agricultural field experiments to compare the yields of different varieties of wheat, for the analysis of data from human clinical trials evaluating the relative effectiveness of competing therapies for disease, or for the analysis of data from environmental studies on the effects of air or water pollution on the appearance of human disease in a region or country are all examples of problems that would fall under the umbrella of “Biometrics” as the term has been historically used. The term “Biometrics” has also been used to refer to the emerging field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition.

2. BIOMETRIC SYSTEM

A biometric system is a real-time identification system which identifies a person by measuring a particular physical or behavioral characteristic and later comparing it to a library of characteristics belonging to many people. Fingerprint and other biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, and wherever the data is to be analyzed, a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data scanned when a user tries to gain access.

2.1. Verification and Identification

There are two different ways to resolve a person's identity: Verification and Identification. Identification means establishing a person's identity Verification involves confirming a person's claimed identity. Each one of these approaches has its own complexities and could probably be solved best by a certain biometric system. It could be noted that verification systems on the other hand are straightforward in operation and may easily be deployed within a broad cross section of applications, as indeed has been the case.

3. POTENTIAL AND CURRENT APPLICATION AREAS

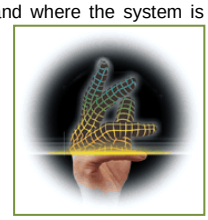
Personal identification numbers are one of the first identifiers to offer automated recognition. It means recognition of the PIN. A biometric cannot be easily transferred between individuals and represents as unique an identifier. It means that verifying an individual's identity can become both more streamlined by the user interacting with the biometric reader and considerably more accurate as biometric devices are not easily fooled. The person to be identified is required to be physically present at the point-of-identification. Identification based on biometric techniques obviates the need to remember a password or carry a token. The critical variable for identification cannot be lost or forged. Presently, biometrics gravitate around the following methodologies –

3.1. Fingerprint verification

There are a variety of approaches to fingerprint verification. Some of them try to emulate the traditional police method of matching minutiae, others are straight pattern matching devices, and some adopt a unique approach all of their own, including ultrasonics. There are a greater variety of fingerprint devices available than other biometric systems at present. Potentially capable of good accuracy fingerprint verification may be

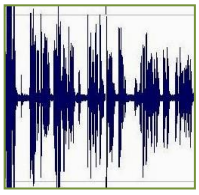
Karpagavalli et al.
Role of multibiometric systems in analysis of biological data,
Indian journal of engineering, 2013, 4(9), 3-7,

a good choice for in house systems where adequate explanation and training can be provided to users and where the system is operated within a controlled environment. It is not surprising that the workstation access application area seems to be based almost exclusively around fingerprints, due to the relatively low cost, small size easily integrated into keyboards and ease of integration.



3.2. Hand geometry

Hand geometry is concerned with measuring the physical characteristics of the users hand and fingers, from a three-dimensional perspective. One of the most established methodologies; it offers a good balance of performance characteristics and is relatively easy to use. This methodology may be suitable where we have larger user bases or users who may access the system infrequently and may therefore be less disciplined in their approach to the system. Hand geometry readers are deployed in a wide range of scenarios, including time and attendance recording where they have proved extremely popular. Ease of integration into other systems and processes, coupled to ease of use makes hand geometry an obvious first step for many biometric projects.



3.3. Voice verification

This is a potentially interesting technique in terms of the amount of voice communication that takes place with regard to everyday business transactions is considered. Some designs have concentrated on wall-mounted readers and others have sought to integrate voice verification into conventional telephone handsets. There have been a number of voice verification products introduced to the market; many of them have suffered in practice due to the variability of both transducers and local acoustics. In addition, the enrolment procedure has often been more complicated than with other biometrics leading to the perception of voice verification as unfriendly in some quarters.

3.4. Retinal scanning

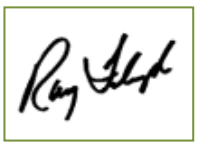
This is an established technology where the unique patterns of the retina are scanned by a low intensity light source via an optical coupler. Retinal scanning has proved to be quite accurate in use but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient for spectacle wearers and for those who avoid intimate contact with the source used for the scan and hence this has a few user acceptance problems although the technology itself can work well.

3.5. Iris scanning

Iris scanning is the less intrusive of the eye related biometrics. It utilizes a conventional camera element and requires no intimate contact between user and reader. In also has the potential for higher than average template matching performance. It has been demonstrated to work with spectacles in place and with a variety of ethnic groups and is one of the few devices that can work well in identification mode.

3.6. Signature verification

Signature verification enjoys a synergy with existing processes that other biometrics does not as people are used to signatures as a means of transaction related identity verification and mostly see nothing unusual in extending this to encompass biometrics. Signature verification devices have proved to be reasonably accurate in operation and obviously lend themselves to applications where the signature is an accepted identifier.



3.7. Facial recognition

Facial recognition devices have been difficult to substantiate in practice and extravagant claims have sometimes been made them. Facial recognition is very attractive from the user perspective and they may eventually become a primary biometric methodology.

3. BIOMETRIC APPLICATIONS

This is an overview of existing and possible future applications of biometrics.

3.1. Access control

Obtaining access to a secured area or system is mostly two-step process identification, the process by which the user professes an identity by providing a username, a pin code or some other form of ID. Authentication, the process of verification or testing to make sure that the user is who he claims to be. Biometrics can be used for both steps, identification requiring a one-to-many search in the templates database and authentication a one-to-one comparison of the measured biometric with the template that is associated to the claimed identity. A lot of commercial, biometric access control solutions are available, and many more are in development. Access control to computer systems fingerprint readers, voice and face recognition software using standard camera and microphone hardware, etc. Door security: doors with biometric locks using iris recognition, fingerprint readers, etc.

3.2. Time and attendance management

The problems with time registration and attendance management are very similar to those encountered with access control. Nowadays most systems identify employees with a pin code or a badge. Using biometric time registration or attendance management avoids fooling and also reduces overhead for security personnel when badges are lost or pin codes forgotten. A number of commercial solutions already exist.

3.3. Surveillance

Screening large crowds for fugitive criminals or missing children, or border control in for example airports can be largely automated using biometrics. The cost of such implementations of biometrics is very high and for existing surveillance systems the success rates vary.

3.4. US-Visit program

The US department of Homeland Security applies fingerprint recognition for border control. Non-US citizens between 14 and 79 years old, entering the United States have all 10 fingerprints taken by electronic means. Japan implemented a similar system under the name J-VIS, scanning both index fingers of foreign visitors. Also the United Arab Emirates implemented a border control system using iris recognition. This type of immigration and border control system is reason for much controversy.

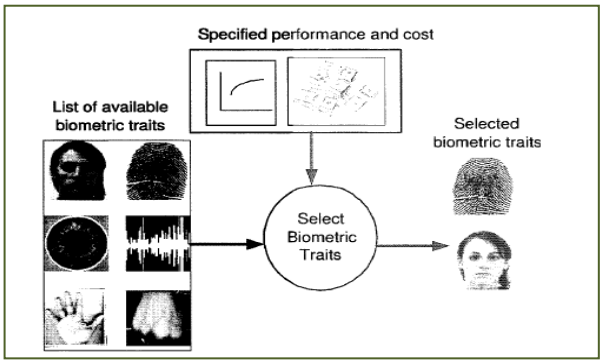
3.5. Multibiometric systems

Multibiometric systems can offer substantial improvement in the matching accuracy of a biometric system depending upon the information being combined and the fusion methodology adopted. Multi biometrics addresses the issue of non-universality or insufficient population coverage. If a person's dry fingers prevent him from successfully enrolling into a fingerprint system, then the

Karpagavalli et al.
Role of multibiometric systems in analysis of biological data,
Indian journal of engineering, 2013, 4(9), 3-7,

availability of another biometric trait, say iris, can aid in the inclusion of this individual in the identity management system. It becomes increasingly difficult for an impostor to spoof multiple biometric traits of a legitimately enrolled individual. If each subsystem indicates the probability that a particular trait is a 'spoof, then appropriate fusion schemes can be employed to determine. Furthermore, by asking the user to present a random subset of traits at the point of acquisition, a Multibiometric system facilitates a challenge-response type of mechanism, thereby ensuring that the system is interacting with a live user.

Multibiometric systems also effectively address the problem of noisy data. When the biometric signal acquired from a single trait is corrupted with noise, the availability of other traits may aid in the reliable determination of identity. Some systems take into account the quality of the individual biometric signals during the fusion process. This is especially important when recognition has to take place in adverse conditions where certain biometric traits cannot be reliably extracted. These systems also help in the continuous monitoring or tracking of an individual in situations when a single trait is not sufficient. For example, a person walking down a crowded aisle can be recognized using his face and gait cues. However, depending upon the distance and pose of the subject with respect to the camera, both these characteristics may not be simultaneously available. Therefore, either of these traits can be used depending upon the situation. A Multibiometric system may also be viewed as a fault tolerant system which continues to operate even when certain biometric sources become unreliable due to sensor or software malfunction, or deliberate user manipulation. The notion of fault tolerance is especially useful in large-scale authentication systems handling a large number of users. Some of the other factors that impact the design and structure of a multi biometric system are described below. Cost benefits: What is the tradeoff between the added cost and the improvement in matching performance? The cost is a function of the number of sensors deployed, the time taken to acquire the biometric data, the storage requirements, the processing time of the algorithm and the perceived convenience experienced by the user.



Multimodal biometric systems utilize different body traits to establish identity

3.6. Determining sources of biometric information

The various sources of biometric information that can be used in a Multibiometric system can be identified. The sources are relevant to the application at hand could be determined. Acquisition and processing sequence: Should the data corresponding to multiple information sources be acquired simultaneously or at different time instances, as the need arises.

4. TYPE OF INFORMATION

Type of information or attributes i.e., features, match scores, decisions, etc. is to be fused. The impact of correlation among the sources of information on the performance of the fusion system can be identified.

4.1. Fusion methodology

To make a business case for multi biometric systems, it is necessary to measure the performance gain as a function of the cost incurred in deploying such a system. The addition of multiple sensors, for example, would increase the cost of the system significantly especially if the user interface has to be altered in order to accommodate new devices. Furthermore, the throughput of the system can potentially decrease if the time taken to acquire the biometric data corresponding to multiple traits is high. While it is possible to quantify the additional cost of sensors and the increased authentication time, it is substantially difficult to quantify the system's ability to deter potential impostors from launching a spoof attack. Similarly, it may not be possible to quantify the time needed number of authentication attempts for user habituation and the potential inconvenience as perceived by the user. In light of this, the benefit of a multi biometric system is often evaluated based on its matching accuracy, the number of users that can be accommodated in the system, the cost of adding new sensors and the additional time required for acquiring and processing multiple traits both during enrollment and authentication. In principle, a large number of traits can be used to improve the identification accuracy. In practice, factors such as cost of deployment, finite training sample size, throughput time and user training will limit the number of traits used in a particular application.

5. SOURCES OF MULTIPLE EVIDENCES

5.1. Multi-sensor systems

In these systems, a single biometric trait is imaged using multiple sensors in order to extract diverse information from multi-instance, multi-sample and multimodal. In the first four scenarios, a single biometric trait provides multiple sources of evidence. In the fifth scenario, different biometric traits are used to obtain evidence e.g spatially registered images. The various sources of information in a multibiometric system: multi-sensor, multi algorithm, multi-instance, multi-sample and multimodal. In the first four scenarios, a single biometric trait provides multiple sources of evidence. In the fifth scenario, different biometric traits are use to obtain evidence. For example, a system may record the two-dimensional texture content of a person's face using a CCD camera and the three-dimensional surface shape of the face using a range sensor in order to perform authentication. The introduction of a new sensor to measure the facial surface variation increases the cost of the multi biometric system (Bendjebbour et al. 2001). However, the availability of multi-sensor data pertaining to a single trait can assist the segmentation and registration procedures also besides improving matching accuracy. A scheme to fuse the fingerprint information of a user can be obtained by using an optical and a capacitive fingerprint sensor (Marcialis et al. 2003). The authors, in their work, indicate that the two sensors provide complementary information thereby resulting in better matching accuracy. The possibility of employing a dynamic sensor selection scheme wherein, were suggested based on the nature of the input data obtained from the two sensors, the information from only one of the sensors may be used to perform recognition (Woods et al.1997; Giacinto et al. 2001). Chen examined the face images of an individual obtained using a thermal infrared camera and a visible light camera. They demonstrate that integrating the evidence supplied by these two images improves matching performance (Chen et al. 2005). Heo also demonstrated the benefits of using thermal infrared and visible light imagery for face recognition (Heo et al. 2004).

5.2. Multi-algorithm systems

Ross reported that texture-based algorithm and a minutiae-based algorithm can operate on the same fingerprint image in order to extract diverse feature sets that can improve the performance of the system. This does not require the use of new sensors and, hence, is cost-effective (Ross et al. 2003). Furthermore, the user is not required to interact with multiple sensors thereby enhancing user convenience. A multi-algorithm system can use multiple feature sets i.e., multiple representations extracted from the same biometric data or multiple matching schemes operating on a single feature set. Lu reported a face recognition system that employs three different feature extraction schemes viz Principal Component Analysis, Independent Component Analysis and Linear Discriminant Analysis to encode a single face image. The authors postulated that the use of different feature sets makes the system robust to a

Karpagavalli et al.
Role of multibiometric systems in analysis of biological data,
Indian journal of engineering, 2013, 4(9), 3-7,

variety of intra-class variations normally associated with the face biometric. Experimental results indicate that combining multiple face classifiers can enhance the identification rate of the biometric system (Lu et al. 2003). Han and Bhanu, presented a context-based gait recognition system which invokes and combines two gait recognition classifiers based on the walking surface (Han et al. 2005). A probabilistic approach is used to combine the participating classifiers. The authors demonstrated that using context information in a fusion framework has the potential to improve the identification rate of the system. The evidence of three different fingerprint matchers to determine the similarity between two minutiae sets was reported (Jain et al. 1999). The three minutiae matchers considered in their system are based on the Hough transform, one-dimensional string matching and two-dimensional dynamic programming. They observe that the matching performance obtained by combining two of the three matchers is comparable to combining all the three matches. Factors such as the correlation between component algorithms, the disparity in their matching accuracies, and the fusion methodology adopted significantly impact the performance obtained after fusion. Ross et al. designed the multi-algorithm fingerprint matcher designed the system utilizes both minutiae and texture information to represent and match two fingerprint images (Ross et al. 2003). The minutiae matching module provides the transformation parameters necessary to align the query image with the template before extracting the texture information from the former. The texture information is represented using ridge feature maps.

5.3. Multi-instance systems

These systems use multiple instances of the same body trait and are also referred to as multi-unit systems in the literature. For example, the left and right index fingers, or the left and right irises of an individual may be used to verify an individual's identity. Multi instance systems are especially beneficial for users whose biometric traits cannot be reliably captured due to inherent problems. For example, a single finger may not be a sufficient discriminator for a person having dry skin. However, the integration of evidence across multiple fingers may serve as a good discriminator in this case. Similarly, an iris system may not be able to image significant portions of a person's iris due to drooping eyelids. The consideration of both the rides will result in the availability of more texture information that can be used to establish the individual's identity in a more reliable manner. Multi-instance systems are often necessary in applications where the size of the system database.

5.4. Multi-sample systems

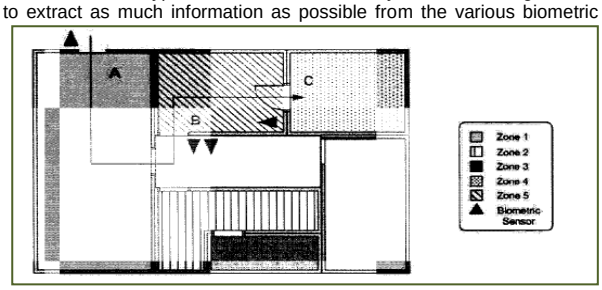
A single sensor may be used to acquire multiple samples of the same biometric trait in order to account for the variations that can occur in the trait, or to obtain a more complete representation of the underlying trait. A face system, for example, may capture and store the frontal profile of a person's face along with the left and right profiles in order to account for variations in the facial pose. Similarly, a fingerprint system equipped with a small size sensor may acquire multiple dab prints of an individual's finger in order to obtain images of various regions of the fingerprint. A mosaicing scheme may then be used to stitch the multiple impressions and create a composite image. One of the key issues in a multisampling system is determining the number of samples that have to be acquired from an individual. It is important that the procured samples represent the variability as well as the typicality of the individual's biometric data. To this end, the desired relationship between the samples has to be established before-hand in order to optimize the benefits of the integration strategy. A face recognition system utilizing both the frontal- and side profile images of an individual may stipulate that the side-profile image should be a three-quarter view of the face (Hill et al.1997; O'Toole et al.1995). Alternately, given a set of biometric samples, the system should be able to automatically select the "optimal" subset that would best represent the individual's variability.

5.5. Multimodal systems

Brunelli and Falavigna reported that some of the earliest multimodal biometric systems utilized face and voice features to establish the identity of an individual. Physically uncorrected traits such as fingerprint and iris are expected to result in better improvement in performance than correlated traits (Brunelli et al.1999). The cost of deploying these systems is substantially more due to the requirement of new sensors and, consequently, the development of appropriate user interfaces. The identification accuracy can be significantly improved by utilizing an increasing number of traits although the curse-of dimensionality phenomenon would impose a bound on this number. Jain and Chandrasekaran reported that the curse-of-dimensionality limits the number of attributes used in a pattern classification system when only a small number of training samples is available. The number of traits used in a specific application will also be restricted by practical considerations such as the cost of deployment, enrolment time, throughput time, expected error rate, user habituation issues, etc (Jain et al. 1982).

5.6. Hybrid systems

Chang et al., made use of the term hybrid to refer to systems that integrate a subset of the five scenarios discussed above (Chang et al. 2005). For example, Brunelli and Falavigna, developed an arrangement in which two speaker recognition algorithms are combined with three face recognition algorithms at the match score and rank levels via a HyperBF network. Thus, the system is multi-algorithmic as well as multimodal in its design. Hybrid systems attempt to extract as much information as possible from the various biometric modalities. Besides the above scenarios, it is also possible to use biometric traits in conjunction with non-biometric identity tokens in order to enhance the authentication performance. For example, Jin noted a dual factor authenticator that combines a pseudo random number with a facial feature set in order to produce a set of user-specific compact codes known as Bio Code (Jin et al. 2004). The pseudo random number and the facial feature sets are fixed in length and an iterated inner product is used to generate the Bio Code. When an individual's biometric information is suspected to be compromised, then the token containing the random data is replaced, thereby revoking the previous authenticator. The use of biometric and non-biometric authenticators in tandem is a powerful way of enhancing security.



Beattie et al. received a scenario in which biometric sensors are placed at various locations in a building in order to impart security to individual facilities/ rooms. The building is partitioned into various zones based on access privileges assigned to different users of the building. The authentication decision rendered at a particular zone may depend on the decisions made previously in other zones (for the same user). Furthermore, in very sensitive zones, a combination of biometric evidences may be used to validate an individual's identity, while in less sensitive zones, a single biometric evidence may be sufficient to establish identity. The fusion scheme used to combine the decisions of multiple sensors can also vary depending upon the zone that a user intends to enter (Beattie et al. 2004). He approved the inclusion of multiple fusion rules involving multiple sensors in a dynamic architecture. The presence of biometric sensors in various zones can also aid in determining an individual's location within the building. The scenario envisioned by Beattie et al., in which biometric sensors are installed at various locations within a building that is partitioned into various zones. The authentication decision rendered at a particular location for a specific user is a function of the decisions generated at other locations previously visited by the same user. Thus, there is an integration of evidence across space and time. Moreover, the fusion rule employed at a particular site can vary depending upon the security level of the associated zone. For example, in the above illustration, a user entering site B has to be verified using two biometric sensors whose decisions may be combined using the AND decision rule.

Karpagavalli et al.
Role of multibiometric systems in analysis of biological data,
Indian journal of engineering, 2013, 4(9), 3-7,

6. CONCLUSION

There are significant privacy and civil liberties concerns regarding the use of devices using biometrics that must be addressed before any widespread deployment. Briefly there are six major areas of concern: they are the problem of storage and methods of storage, Vulnerability Confidence, Authenticity, Linking and Ubiquity. With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive personal data. By replacing personal identifications, biometric techniques can potentially prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token-based methods of identification like passports and driver's licenses may be forged, stolen, or lost. Thus biometric systems of identification are enjoying a renewed interest. There are many views concerning potential biometric applications, some popular examples being - ATM machine use - Most of the leading banks are considering using biometrics for ATM machine and as a general means of combating card fraud. Workstation and network access and Travel and tourism - Many people hold the vision for a multi application card for travelers which, incorporating a biometric, would enable them to participate in various frequent flyer and border control systems as well as paying for their air ticket, hotel room, hire care etc., all with one convenient token.

REFERENCES

1. Beattie M, Kumar B V K Vijaya, Lucey S, Tonguz O, Building access control using coordinated biometric verification. *In Biometrics:Challenges arising from Theory to Practice(BCTP) Workshop Proceedings*. 2004
2. Bendjebbour A, Delignon Y, Fouque I, Samson V , Pieczynski W, Multisensor image segmentation using Dempster–Shafer fusion in Markov field context, *IEEE transactions on geoscience and remote sensing*, 2001, 39(8), 1789–1798
3. Brunelli Roberto**,** Falavigna Daniele **,** Person identification using multiple cues, *Pattern Analysis and Machine Intelligence, IEEE Transactions* , 1999,17(10) ,955–966
4. Chang K I, Bowyer K W, Flynn P J, Adaptive rigid multi-region selection for handling expression variation in 3D face recognition. *In Proc. IEEE Workshop on Face Recognition Grand Challenge Experiments*, Washington, DC, USA 2005,157
5. Chen Y, Wang J Z, Krovetz R, Clue: Cluster-based retrieval of images by unsupervised learning, *IEEE Trans. Image Process*, 2005, 14, 1187–1201
6. Giacinto G, Roli F, Design of effective neural network ensembles for image classification, *Image and Vision Computing Journal*, 2001, 19, 697-705
7. Han J, Bhanu B, Performance prediction for individual recognition by gait, *Pattern Recognition Letters*, 2005, 26, 615-624
8. Heo J, Kong S, Abidi B, Abidi M, Fusion of visual and thermal signatures with eyeglass removal for robust face recognition, *Proceedings of the Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'04)*, Washington, July, 2004, 8,122
9. Hill H, Schyns P, Shigeru A, Information and viewpoint dependence in face recognition, *Cognition,* 1997,62 ,201 – 222
10. Jain A K, Hong L, Kulkarni Y, A multimodal biometric system using fingerprint, face and speech, *In: Proceedings of the Second International Conference on Audio- and Video-based Biometric Person Authentication, Washington DC*, 1999a, 182-187
11. Jain AK, Chandrasekaran B, Dimensionality and sample size consideration in pattern recognition practice. In: P.R. Kdshnaiah and L.N. Kanal, Eds., Handbook *of Statics*, 1982, Vol. 2. North-Holland, Amsterdam, 835-855
12. Jin A, Ling D, Goh, A, Personalised cryptographic key generation based on FaceHashing, *Computers & Security*, 2004, 23, (7), 606−614
13. Lu J, Plataniotis K N, Venetsanopoulos A N, Face recognition using kernel direct discriminant analysis algorithms. *IEEE Transactions on Neural Networks*, 2003, 14, 117-126.
14. Marciali G L, Roli F, Experimental results on fusion of multiple fingerprint matchers. in: Kittler, J., Nixon, M.S. (Eds.), *Proc. 4th Internat. Conf. on Audio and Video-Based Person Authentication AVBPA03.* Springer LNCS2688, 2003a,814–820
15. O'Toole A J, Abdi H, Valentin D, Face recognition with a neural network. In M. A. Arbib (Ed.), The *Handbook of Brain Theory and Neural Networks*. Cambridge:Bradford Books/MIT Press, 1995
16. Ross A, Jain A K, Information fusion in biometrics*, Pattern Recognition Lett.,* 2003, 24 (13), 2115–2125
17. Ross A, Jain AK, Reisman J, A hybrid finger print matcher. *Pattern Recognition*, 2003, 36 (7), 1661–1673
18. Woods K, Kegelmeyer W P, Bowyer K, Combination of multiple classifiers using local accuracy estimates, *IEEE Transactions on Pattern Analysis and Machine Intelligence* 1997,19 (4), 405-410

Karpagavalli et al.
Role of multibiometric systems in analysis of biological data,
Indian journal of engineering, 2013, 4(9), 3-7,