Australian Journal of Basic and Applied Sciences, 9(16) Special 2015, Pages: 354-360

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Multimodal Biometrics: A Survey

[1]T.S. Sasikala and [2]Dr. J. Jeya A Celin

[1]*Department of Computer Science and Engineering, Noorul Islam University, India.*
[2]*Department of Information Technology and Engineering, Noorul Islam University, India.*

ARTICLE INFO

Article history:
Received 20 January 2015
Accepted 02 April 2015
Published 20 May 2015

Keywords:
Biometrics Features
Multimodal Biometrics
Fusion

ABSTRACT

Authentication of users is an essential and difficult task to achieve in all systems. The biometric improves the capability to recognize persons. The objective of a biometric authentication system is to recognize a person based on physiological or behavioral characteristics. In many real-world applications, unimodal biometric systems often face significant limitations due to sensitivity to noise, intra class variability, data quality, non-universality, and other factors. Multimodal biometric systems overcome some of these limitations. "Multimodal biometric systems in general provide better accuracy and performance when compared to unimodal biometric systems". The main goal of a multimodal biometric system is to provide a high level of security. This paper is focused on the detail about developing a multimodal biometrics system. Fusion of various biometric triats is performed using various methods discussed below.

To Cite This Article: T.S. Sasikala and Dr. J. Jeya A Celin., Multimodal Biometrics: A Survey. ***Aust. J. Basic & Appl. Sci.,*** *9(16): 354-360, 2015*

INTRODUCTION

Today in the global world as the personal and institutional security requirements increase , a person has to remember several passwords, pin numbers, account numbers, voice mail access numbers and other security codes which is sometimes impossible to memorize or remember it. However passwords have their own weakness. The weak passwords can be guessed and strong passwords can be broken and some time passwords can be shared. It is recommended that people should not use the same password for more than one application and should change them regularly. More over tokens such as smart cards, photo ID cards, physical keys, ATM cards etc. can be lost, stolen, duplicated, or left at home. Biometric authentication is the idle solution to all these requirements; it holds the promise of fast, ease-to-use, accurate, reliable, and less expensive authentication for variety of applications.

The word BIOMETRIC is derived from the Greek letters ‘bios‘ and ‘metric‘; which means; life and measurement respectively, directly translates into “Life Measurements” Pooja and Ashish (2012). Biometrics is the automated use of physiological or behavioral characteristics to determine or verify identity. Biometrics is best defined as measurable physiological and or behavioral characteristics that can be utilized to verify the identity of an individual.

The history of biometrics can be traced back as far as the fourteenth century when it was used by merchants in China where thumbprints and other anatomy measurements were used as a method for identifying and keeping track of customers. A new method named Bertillionage was developed by Alphonse Bertillion during the later part of 19th Century for identifying people by taking measurement of their body Pooja and Ashish (2012). Biometric technologies provide user friendly and reliable control methodology for access to computer systems, networks and workplaces Dugelay et a.l(2002). The majority of research is aimed at studying well-established physical biometrics such as fingerprint, iris scans etc. Behavioral biometrics systems are usually less established, and only those which are in large part based on muscle control such as keystrokes, gait or signature are well analyzed Roman and Venu(2008).

Biometric authentication system works on two basics Identification and Verification**.** In the identification mode the system validates a person’s identity by comparing the captured biometric data with the stored template present in the database. The system conducts a one-to-many comparison to identify whether the user is genuine or imposter. In the verification mode, the system validates a person’s identity by comparing the captured biometric data with his or her own biometric template(s) stored in the system database. The system conducts a one-to-

Corresponding Author: Sasikala T.S., Research Scholar, Department of CSE, Noorul Islam University, Thuckalay, Kanyakumari District, Tamil Nadu, India.
E-mail: Sasikalaselva2012@gmail.com, sksksv@rediffmail.com.

one comparison to determine whether the claim is true or not. Techniques used in biometric requires that the person to be identified or verified must physically present in the spot.

Usually Physiological techniques are based on physical characteristics. Examples include fingerprint recognition, iris recognition, face recognition, hand geometry. Whereas, Behavioral techniques are based on the things you do, that is trained act or skill that the person unconsciously does as a behavioral pattern. Examples include voice, signature recognition, Gait recognition etc.

1. Biometric Characteristics:

Hand geometry:

Hand geometry based biometric systems exploit features on the human hand to perform identity verification. A number of techniques for personal verification based on hand geometry features have been proposed in the literature. In general users are required to place their hand on flat surface fitted with pegs to minimize variations in the hand position. Hand geometric systems use an optical camera to capture two orthogonal two dimensional images of the palm and sides of the hand, offering a balance of reliability and relative ease of use.

Image acquisition can be done in three different ways:

- Constrained and contact based: These systems employ pegs or pins to constrain the position and posture of hand.
- Unconstrained and contact based: These systems employ users to place their hand on flat surface or a digital scanner.
- Unconstrained and contact-free: This approach is believed to be more user-friendly and have recently received increased attention from biometric researchers.

A hand recognition system based on various fingers widths, heights, deviations and angles are presented in the literature. For recognition purpose some techniques may use the palmer surface, some other system use the dorsal surface, lateral hand surface etc. In most of the systems, the hand image was captured using 45 to 180 dots per inch (DPI) scanners. A recent trend in hand-based biometric systems is oriented towards a platform-free, non-contact image acquisition setup. Hand geometry system based on an innovative contactless approach with No guidance pegs for hand image acquisition is also proposed. Hand geometry technique by restricting pegs is proposed in Xiong *et al*. (2005). Neural Network based Hand geometry application use two different classifiers: a support vector machine, and a neural network. A Support Vector Machines (SVM) is a very spread classifier because it generally provides better generalization performance when the amount of data is small. The geometrical parameters of the hands have been also classified with a Multi-Layer Perceptron (MLP). It has been trained as follows: when the input data belongs to a genuine person, the output is fixed to 1. When the input is an impostor person, the output is fixed to –1.

Fingerprint:

Fingerprints have been used for personal identification for many centuries, the matching accuracy using fingerprints has been shown to be very high but fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors, aging, environmental, or occupational reasons Jain and Ross(2004). Personal authentication using both finger geometry and dorsal finger knuckle surface features was investigated. Hand-print verification system utilizing whole hand skin image for recognition, features were extracted in different parts of the hand, and final decision was made in a matching score level fusion manner . Fingerprint-based biometric system also extract the minutiae feature and the texture feature of the fingerprints, and integrated them at decision level using the Neyman-Pearson rule .

Face:

Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall analysis of the face image that represents a face as a weighted combination of a number of canonical faces. In order for a facial recognition system to work well in practice, it should automatically:

- Detect whether a face is present in the acquired image
- Locate the face if there is one and
- Recognize the face from a general viewpoint (i.e., from any pose).

The approach towards 3D face recognition is based on computation of the surface curvature, which is subsequently used for the localization of facial features the construction of Extended Gaussian Images or the extraction of local Points. Optimal decision fusion by “AND” rule and “OR” rule was developed , and they can be employed to combine 2D face texture and 3D face shape information at decision level Tao *et al*.(2007).

Signature:

Signature verification provides an alternative for authentication other than physical biometric features. The production of the signature and the matching process can be done using variety of techniques, such as hidden Markov models and eigen analysis . Signatures are composed of special characters and

flourishes, which make them most of the time unreadable. Besides, intrapersonal variations and differences make the analysis of these signatures as complete images and not as letters and words important and unique. That is why signatures have been accepted in government, legal, and commercial transactions as a method of verification. There are two different types of signature verification: offline and online. Offline takes only a signature's image and analyses it, and then compares it to the stored template to measure similarity. In the case of online method various features that are determined by the signing method are evaluated. However, online techniques cannot be applied for verifying signatures on documents or bank cheques.

Signature based technologies measures the speed and pressure of an user when signing his or her name-not what the signature itself looks like. It is based on measuring speed, pressure and angle used by the person generating a signature. Also writer speed decreases with increasing in a signing task.

Traditional signature verification systems usually use digitizing tablets or scanners to collect handwritten signatures. The signatures are time sequences with variable length. Signature verification system utilizes techniques like hidden Markov models (HMM) and dynamic time warping (DTW) to deal with the variable length data Yang Fan and Ma Baofeng(2007a). The authors presented a method to fuse HMM and DTW for on-line signature verification Aguilar *et al*. (2005). A multi-expert verification system can also be used for signature verification. Signatures verification based on geometric extrema for more stable results is proposed by Lee and Park (2006). In Camera-based signature verification system the pen-tip was tracked using a Kalman filter or particle filter and performed curve matching using dynamic programming munich and Perona(1998). In Signature verification system incorrect pen-tip positions can be eliminated and correct pen-tip positions can be extracted using a mechanism based on K-means clustering algorithm and particle filtering Cheng *et al*. (2012) . Also, analysis of signature image process is done through curvelet transform. The major problem faced with this technology is that a person's signature changes with time and is highly affected by the physical and emotional conditions of the signature. As a matter of fact, even successive signatures by the same person can be significantly different.

Ear Biometrics:

The possibility of identifying people by the shape of their outer ear was first discovered by the French criminologist Bertillon. First ear recognition system was conducted by the American police officer Alfred Iannarelli. He also conducted studies on twins and triplets, discovering that ears are even unique among genetically identical persons. The German criminal police use the physical properties of the ear in connection with other appearance-based properties to collect evidence for the identity of suspects from surveillance camera images. Authors Abaza and Ross (2010) proved that the shape of the outer ear evolves during the embryonic state from six growth nodules, left and the right ear are also not symmetric. The ear can easily be captured from a distance, even if the subject is not fully cooperative. The characteristic appearance of the human outer ear is formed by the outer helix, the ntihelix, the lobe, the tragus, the antitragus and the concha. The numerous ridges and valleys on the outer ear's surface serve as acoustic resonators.

It is clear that the recognition rate of ear is not affected by age, but the size of ear slightly changes by age. Chen and Bhanu (2005) propose an approach which works on profile images and is sensitive to any kind of rotation, scale and pose variation. In their later ear detection approaches they detected image regions with a large local curvature with a technique they called step edge magnitude. Ear detection is performed using contour lines of the ear Ray transform approach detects the ear in different poses. An ear detection method fuses range images and corresponding 2D color images Islam *et al*. (2007).

Gait:

Identification of humans based on their way of walking is referenced to as gait biometrics. A person will perform his or her walking pattern in a fairly repeatable and characteristic way, sufficiently unique that it is possible to recognize a person at a distance by their gait. Usage of gait biometric in individual identification is a rather new and encouraging research area in biometrics. Gait has been shown to be an efficient biometric feature for human identification at a distance requiring no cooperation from the observed individual, and functionality from distance, using non-expensive low resolution cameras, are the benefits that have been dragging enormous attention to gait biometric. However, it should be noted that, gait pattern in humans can be greatly affected by changing of clothes, shoes, or even emotional states. But gait is a dynamic feature of humans which has been proven to have strong recognition abilities. The initial gait sequence is processed so as to extract the geometric gait features and the soft biometric features. Geometric gait feature is extracted using Radial Integration Transform (RIT).

Generally techniques used for gait recognition, can be divided into two classes; model-based approaches and model-free approaches. In model-based approaches, a model of human body or walking human motion is provided. As input and during the recognition procedure, model parameters are updated frame to frame. In model-free approaches the statistical criterions extracted directly

from the walking frame sequences, are used for recognition. Also, there are some hybrid works combining both model-based dynamic cues and model-free static cues. Human ID at a Distance Project uses gait to help identify terrorists from a distance. Additionally, it is difficult for one to deliberately copy someone else's way of walking. Having said all of this, gait recognition is still in its infancy and has not faced many tests, especially for potential attacks.

Regarding the situations of view, there are three cases in the practices: fixed-view gait recognition, cross-view gait recognition and multi-view gait recognition. Cross-view and multi-view gait recognitions are achieved based on a novel view transformation model (VTM), For multi-view gait recognition and 3D gait model based methods multi-layer perceptron(MLP) method is used Kusakunniran *et al*.(2009).

Based on fact that gait is a unique biometric data for each person, scientists have realized that it is possible to make gender classification from gait. In this study, the feature vectors were extracted from the RIT's and CIT's of the binary silhouette images of human gait scenes. These feature vectors were used in the Support Vector Machine (SVM) and Linear Vector Quantization (LVQ) classifiers for gender recognition.

Odor:

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. Medical researcher Lewis Thomas first suggested a link between immunity and body smell in the middle of 1970 [44]. Human sweat contains a mixture of odorants with trigeminal as well as olfactory properties. Olfaction has an extremely high importance in the human being. It is one of the five main senses: Sight, Smell, Taste, Hearing and Touch (The senses 2003).

Main operations of olfaction can be divided roughly in five parts: sniffing, reception, detection, recognition, and cleansing. The olfaction begins with sniffing that mixes the odorants into a uniform concentration and delivers these mixtures to the mucus layer in the upper part of nasal cavity. Next these molecules are dissolved in this layer and transported to the cilia of the olfactory receptor neurons. Reception process includes binding of these odorant molecules to the olfactory receptors. Odorant molecules are binded temporarily to proteins that transport molecules across the receptor membrane with simultaneous stimulation of the receptors During this stimulation the chemical reaction produces an electrical stimulus. These electrical signals from the receptor neurons are transported to the olfactory bulb. From the olfactory bulb the receptor response information is forwarded to the olfactory cortex (detection). Odor recognition part takes place namely in the olfactory cortex. Then the information is transmitted to the cerebral cortex. Remind that there are no individual receptors or parts of the brain capable to recognize specific odors. The brain is key component associated the collection of olfactory signals with the specific odor . Cleansing finishes the olfaction process. For this purpose the breathing fresh air removing of odorant molecules from the olfactory receptors is required.

Voice:

Voice is a combination of physiological and behavioral biometrics. The features of an individual's voice is based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in synthesis of the sound. These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions emotional state etc. There are two modes of voice recognition namely text dependent and text independent.

In the case of text dependent speech the user presents a password or a phrase that is programmed into the system. Text dependent speech recognition is used in applications where a lot of access based security systems use speech as a way of blocking unwanted individuals and most of the speaker verification system of this types uses a concept of Hidden Markov Model (HMM). Performance of Voice biometrics in improved using MFCC based techniques Rishiraj Mukherjee *et al*. (2012). Whereas in the case of text independent speech the user is not aware of about the speech and it is based on the situation or randomly chosen phrase needs to be presented and most of the speaker verification methods of this types uses vector quantization and applications of HMM Danko Komlen *et al*. (2011). Recognition can be performed on a closed or open set, depending on the possibility of using a system on an unknown user. The closed set recognition system should be able to make a rejection when trying to identify unknown users, while the open s*et al*ways classifies a sample. For practical application text-independent methods are more important. Such a system can be built with little or even with no awareness of the speaker, and can thus be used for forensic purposes. Both text dependent and text independent speaker verification methods compares the similarities and differences between the input voice and the stored voice states to produce decision about the recognition Vector quantization (VQ) and GMM are conventional and successful methods for voice recognition.

Iris:

Iris is the ideal part of the eye in human body. No two irises are alike even for identical twins, Iris is the highly protected, internal organ of the eye. Iris contains many distinctive features such as furrows,

ridges and rings etc. It is the annular region of the eye bounded by the pupil and the sclera on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect artificial irises (e.g., designer contact lenses) the speaker recognition approaches. Iris technology provides greater unique identification. The first successful iris recognition algorithm was proposed by Daugman (1993). He utilizes odd and even Gabor filters for iris feature extraction.

2. Why Multimodal Biometrics:

During early days biometric systems that use only one biometric parameter were very common. Few years ago, researchers proposed the deficiencies appeared in these unimodal systems like: Noise in the acquired image, Intraclass variations, Inter-class similarities, Non-universality and Spoof attacks It is also estimated that 5% of the population does not have legible fingerprints Pooja and Ashish (2012), a voice could be altered by a cold and face recognition systems are susceptible to changes in ambient light and the pose of the subject. Fingerprint and iris technologies have outlier cases whereby the system cannot use or enroll the biometric due to injury, medical condition and/or physiological condition. To overcome the limitations of unimodal biometrics we go for multimodal biometrics.

To boost up the security of biometric systems, multibiometrics is a good choice. Multimodality is not only the usage of more than one physiological or behavioral characteristic to identify an individual, but also includes multisensor, multi algorithm, multi-instance and multi-sample. The features offered from several unimodal biometric systems can be fused at different levels. Fusion is done by running two (or more) biometric inputs against two (or more) different algorithms, to arrive at a decision. Stronger biometric is used in applications, where the identity of thousands of people need to conjunction with a weaker biometric, the result is not be authenticated at a time. Moreover, multibiometrics can improve the matching accuracy of a recognition system. Multimodal techniques usually rely on fusion of scores obtained by unimodal classifiers, ignoring the actual information conveyed by the two modalities Lupu *et al*. (2007).

Multimodal biometric system is more strong than unimodal ones. It takes advantage of multiple biometric traits to improve the performance in many aspects including accuracy, noise resistance, universality, spoof attacks and reduce performance degradation in huge database applications.

A multimodal biometric systems with enhanced recognition .0precision and population coverage by using fingerprint and iris was proposed by Tsalakanidou (2005). Two multimodal biometric verification system models based on fingerprint, palm print and hand geometry was proposed and better Receiver Operation Characteristics (ROC) is obtained by yang and Ma Baofeng (2007b). Matching score level fusion applied on eigenfinger and eigen palm features is proposed by Ribaric and Fratric(2005).

A biometric system of palmprint recognition using rank level fusion was also developed by Ajay kumar and sumit shekhar (2013). A multimodal biometric system using fingerprint and iris features use a hybrid approach based on: 1) fingerprint minutiae extraction and 2) iris template encoding through a mathematical representation of the extracted iris region. This approach is based on two recognition modalities and every part provides its own decision. The final decision is taken by considering the unimodal decision through an "AND" operator Besbes *et al*. (2008).

3. Modes of Operation:

A multimodal biometric system can operate in one of three different modes: serial mode, parallel mode, or hierarchical mode. In the serial mode of operation, the output of one biometric trait is typically used to narrow down the number of possible identities before the next trait is used. This serves as an indexing scheme in an identification system. For example, a multimodal biometric system using face and fingerprints could first employ face information to retrieve the top few matches and then use fingerprint information to converge onto a single identity. In the case of parallel mode information from multiple traits is used simultaneously to perform recognition. In the serial operational mode. In the hierarchical scheme, individual classifiers are combined in a treelike structure.

Fusion of multimodal biometrics can be done in three categories: feature extraction level fusion, matching score level fusion and decision level fusion. In a multibiometric system, decision level fusion combined the recognition results of all biometric matchers. As an important fusion method, commonly used decision fusion strategies include majority voting, plurality voting, "AND" and "OR" rules, behavior knowledge space, Dempster-Shafer technique and Neyman-Pearson scheme. Multimodal biometric system combines fingerprint, face and speech at the decision level, whose decision rule is Neyman-Pearson rule.

A new approach for appearance-based multi-modal recognition that does not require a subject's cooperation called as RJSOM method. We use neural

network based self organizing maps for dimensionality reduction as a part of RJSOM method. Generally, in a multimodal biometric system that uses different biometric traits are possible various levels of fusion: fusion at the sensor level, feature extraction level, matching score level or decision level. In multimodal biometrics, the fusion scheme can be classified as sensor level, feature level, match score level, rank level and decision level. Multibiometric system integrates information at the following two categories Radha and Kavitha (2012).

(1) Prior to matching fusion: In this category, fusion integrates the information of biometric before matching.

This includes the following fusion levels.

(i) Sensor level fusion**:** this system fuse raw data obtained from the sensors without any feature extraction and represented as a single unit. This level of fusion is also known as data level fusion or image level fusion.

(ii) Feature level fusion: Data obtained from different sensors are first subjected to feature extraction algorithms and the feature vector that is subsequently used for recognition.

(2) After matching fusion: In this category, fusion integrates the information of biometric after matching. This includes the following fusion levels.

(i) Match-score level fusion: Features extracted from individual biometric modalities are first matched to compute the corresponding match scores. Match scores obtained from different biometric systems are then combined to generate a fused match score.

(ii) Decision level fusion**:** Decisions of individual biometric classifiers are fused to compute a combined decision. This level of fusion is also known as abstract level fusion because it is used when there is access to only decisions from individual classifiers.

(iii) Rank level fusion: Rank level fusion involves combining identification ranks obtained from multiple unimodal biometrics. It consolidates a rank that is used for making final decision.

Many approaches exist for integrating multiple modalities. Fusion approaches can be distinguished in two ways. First of all, fusion could be carried out at different levels. Modalities could be combined at the feature level, the matching level, or the decision level. Secondly, fusion could be based on rules or based on machine-learning approaches . Rule-based approaches include simple sum, max score, and min score. Machine-learning approaches include support vector machines, minimum cost Bayesian classifier, fisher's linear discriminant, decision trees, and multilayer perceptron Faundez-Zanuy (2005)

There are three types of multimodal biometric system. The first type is known as transformation-based. Here the matching scores are normalized (transformed) to place them on a comparable scale. There are several ways to implement the fusion of different matchers, such as sum, product, max, mean, weighted sum, etc. Besides choosing the best fusion strategy, the use of weights to indicate the importance of the matching scores provided by each biometric trait should also be considered. The second type of fusion is called density-based, and it relies on the estimation of the joint densities of the matching scores, and the fusion is carried out by statistical tests, such as the likelihood ratio test. This type of fusion scheme achieves good performance if the densities can be well learned, given that a large number of representative training matching scores are available. The third strategy is classifier based. With this strategy the scores produced by each biometric system are considered as features to feed a classifier. In such a case, each input pattern should be labeled as either genuine or an impostor. A review of the literature reveals several works using classification strategies such as neural networks, k-NN, quadratic classifiers, and support vector machines(SVM).

4. Factors Affecting The Accuracey Of Biometric Measurement:

The performance of the Biometric system is measured in terms of error rates (FAR, FRR, EER and GAR).

- False Rejection Rate (FRR): The valid user may be rejected as an invalid user. This must be low to achieve good Performance.
- False Acceptance Rate (FAR): The Non-authorized user is accepted as authorized user while authentication. In a good authentication system this rate must be low.
- Equal Error Rate (ERR): This can be determined by the ratio FRR: FAR.
- Genuine acceptance Rate (GAR) - It is used to measure the genuine acceptance rate of a valid user.

Performance of a biometric verification system can be evaluated using a Receiver Operator Curve (ROC). ROC is a plor of FMR against FNMR for various thresholds

Conclusion:

In this survey, authors have presented both the behavioural and physiological behaviour for personal identification and for verification. Disadvantages of unimodal biometrics and advantages of multimodal biometrics are examined. Fusion of various unimodal modalities are also examined. In future reasearchers are directed at increasing the overall accuracy of identification and verification system.

REFERENCES

Abaza, A., A. Ross, 2010. ‘Towards understanding the symmetry of human ears: a

biometric perspective'. Fourth IEEE Int. Conf. on Biometrics: Theory Applications and Systems (BTAS).

Aguilar, F., J. Krawczyk, S.O. Garcia, A.K. Jain, 2005.: 'Fusion of local and regional approaches for on-line signature verification', Int. Workshop Biometric Recognit. Syst., 3781: 188-196.

Ajay kumar and sumit shekhar, 2013. 'Palmprint recognition using rank level fusion', Department of Computing, The Hong Kong Polytechnic University, Hong Kong Department of Electrical and Computer Engineering, University of Maryland, College park, USA.

Besbes, F., H. Trichili, B. Solaiman, 2008.'Multimodal biometric system based on fingerprint identification and iris recognition', In: Third Internat. Conf. on Inf. Comm. Technol.: From Theory Appl., ICTTA 2008, pp: 1-5.

Chen, H., B. Bhanu, 2005. 'Contour matching for 3D ear recognition'. Proc. Seventh IEEE Workshop on Applications of Computer Vision (WACV/ MOTION).

Cheng, H.-Y., C.-L. Lin, C.-C. Yu, V. Gau, 2012." Video-based signature verification and pen-grasping posture analysis for user-dependent identification authentication", IET.

Danko Komlen, Tomislav Lombarovi´c, Mario Ogrizek-Toma˘s, Denis Petek and Andrej Petkovi, 2011. 'Text Independent Speaker Recognition Using LBG Vector Quantization', MIPRO 2011, May 23-27, Opatija, Croatia.

Daugman, J.G., 1993. 'High Confidence Visual Recognition of Persons by a Test of Statistical Independence'. IEEE Trans. PAMI, 15(11).

Dugelay, J-L., J-C. Junqua, C. Kotropoulos, R. Kuhn, F. Perronnin and I. Pitas, 2002. 'Recent advances in biometric person authentication', IEEE Int. Conf. on Acoustics Speech and Signal Processing (ICASSP), Special Session on Biometrics, Orlando, Florida.

Faundez-Zanuy, M., 2005.' Data fusion in biometrics', IEEE Aerospace and Electronic Systems Magazine, 20(1): 34-38.

Islam, S., R. Davies, M. Bennamoun, A. Mian, 2011.: 'Efficient detection and recognition of 3D ears', Int. J. Comput. Vis., 95: 52-73.

Jain, A.K., A. Ross, 2004. ' Mutlibiometric Systems', Communications of the ACM, 74.

Kusakunniran, W., Q. Wu, H. Li, J. Zhang, 2009. 'Multiple views gait recognition using view transformation model based on optimized gait energy image'. In: IEEE Internat. Conf. on Computer Vision.

Lee, K. and H. Park, 2003. 'A new similarity measure based on intra-class statistics for biometric systems', ETRI Journal NSTC committee on technology and subcommittee on Biometrics.

Lupu, C., V. Lupu, 2007.' Multimodal Biometrics for Access Control in an Intelligent Car', IEEE.

Munich, M.E., P. Perona, 1998. 'Camera-based ID verification by signature tracking', Lect. Notes Comput. Sci., 1406: 782-796.

Pooja Shelke, Ashish Badiye, 2012. 'Biometrics for Enhancement of Security Standards', International Journal of Advanced Research in Computer Science and Software Engineering.

Radha, N., A. Kavitha, 2012. 'Rank Level Fusion using Fingerprint and Iris Biometrics', Indian Journal of Computer Science and Engineering (IJCSE), 2(6).

Ribaric, S. and I. Fratric, 2005. 'A biometric identification system based on eigenpalm and eigenfinger features', IEEE Trans. Pattern Anal. Mach. Intell., 27(11): 1698-1709.

Rishiraj Mukherjee, Tanmoy Islam, and Ravi Sankar, 2012. 'TEXT DEPENDENT SPEAKER RECOGNITION USING SHIFTED MFCC', IEEE.

Roman, V. Yampolskiy, Venu Govindaraju, 2008. 'Behavioural biometrics: a survey and classification', Int. J. Biometrics, 1(1): 81.

Tao, Q., R. van Rootseler, R. Veldhuis, S. Gehlen and F. Weber, 2007. 'Optimal decision fusion and its application on 3d face recognition', Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, Darmstadt, Germany, GI-Edition, pp: 15-24.

Tsalakanidou, F., F. Forster, S. Malassiotis, M.G. Strintzis, 2005. 'Real-time acquisition of depth and color images using structured light and its application to 3D face recognition'. Real-Time Imaging, 11(5-6): 358-369, Special Issue on Multi-Dimensional Image Processing.

Xiong, W., K.A. Toh, W.Y. Yau, X. Jiang, 2005. 'Model-guided deformable hand shape recognition without positioning aids', Pattern Recognition, 38(10): 1651-1664.

Yang Fan, Ma Baofeng, 2007. 'Two models multimodal biometric fusion based on fingerprint', palm-print and hand-geometry. In: The First Internat. Conf. on Bioinf. Biomed. Eng., pp: 498-501.

Yang F and Ma B, 2007. 'A new mixed-mode biometrics information fusion based-on fingerprint, hand-geometry and palm-print', in Proc. 4th Int. IEEE Conf. Image Graph., pp: 689-693. DOI: 10.1109/ICIG.2007.39.