A Review on Unimodal and Multimodal Biometric Systems

Krishnakumari y,
M.Tech Student,
Computer Network Engineering,
Dept. of CSE,
BNM Institute of Technology
Banglore-560070,

Savitha G,
Associate Professor,
Dept. of CSE,
BNM Institute of Technology
Bangalore-560070,

Abstract: **Biometrics is a method to verify the identity of a person based on psychological characteristics or behavioral characteristics. Examples of biometrics are fingerprints, iris, face, ear, voiceprint, palm print, signature, and handwriting or keystrokes patterns. Biometric systems are classified into two types: (1) Unimodal biometric system (2) Multimodal biometric system. There is a limited accuracy in the unimodal biometric system. Accuracy can be improved by using multimodal biometric system. Two or more biometric traits are used in multimodal biometric system. Here we present characteristics of biometrics, comparison of biometric modalities, difference between unimodal and multimodal biometrics, limitations of unimodal biometrics, fusion levels in biometrics.**

Keywords— *Biometrics, Unimodal biometrics, Multimodal biometrics, Fusion levels, Recognition methods.*

I. INTRODUCTION

Based on physiological or behavioral characteristics, biometric systems are used to recognize a person. Some of the examples of biometrics are face, fingerprint, hand geometry, iris, retinal, signature and voice. To obtain highly secure personal identification and verification details, biometric systems are widely used. The need of identification and verification technologies is very important as the level of security breaches and transaction fraud increases.

To provide confidential financial transactions and personal data privacy, biometrics is used. Biometrics is used in federal, state and local governments, in military and commercial applications. And also in secure electronic banking, government IDs, retail sales, health and social services are using these technologies. Authentication based applications include network, data protection, remote access to resources, workstation, transactions and web security. To provide healthy growth of the global economy, electronic transactions are essential in biometrics. Trust in these electronic transactions is essential to the healthy growth of the global economy. Biometrics is integrated with other technologies such as smart cards, encryption keys and digital signatures. Biometrics is used in our daily lives. Biometric systems are more accurate and convenient for authentication and identification of a person.

There are three different types of authentication for security. They are *something you know* –it provides a PIN, password, or details of person's information, *something you have* –it includes a smart card, card key or secure ID card and *something you are* –which provides biometric information. Among these, biometric systems provide secure and convenient authentication tool and it is not able to stolen, barrowed or forgotten and forging biometric information is very impossible.

II. GENERAL BIOMETRICS TECHNOLOGY

A. Processing phases of biometrics

There are three different processing phases are available in biometrics: they are (1) Enrollment phase (2) Verification phase and (3) Identification phase.

- *Enrollment Phase*

In this phase, template of the individual person images is stored in the database to check person's identity. Using image of that person, features are extracted.

- *Verification Phase*

In this phase, the person is verified with his template which is available in the database by comparing person's captured data.

- *Identification Phase*

In the identification phase, the system will store all user's details. So the system identifies an individual by searching the templates of all users in the system. The system performs one to many comparisons to verify an individual identity, if it is enrolled in the system record.

B. Working of Biometric system

The block diagram of biometric system as shown in figure 1 and its working as follows:

- Sensor Module: In this module, different sensors are used to capture biometric data of the individual.
- Preprocessing: Here, to remove noise from the image, filters are used. Image is converted into requires size that is the captured image is preprocessed.
- Feature Extraction: In this module, once the image is captured and preprocessed from the sensor module and preprocessing module respectively. Then features are extracted from the image using feature extraction module.
- Matching Module: In this module, as we know template of the individual data is stored in the database. So the comparison between the features extracted from the input data and the template stored in the database are performed.
- System Database Module: In this phase, templates of all users are stored in the database.

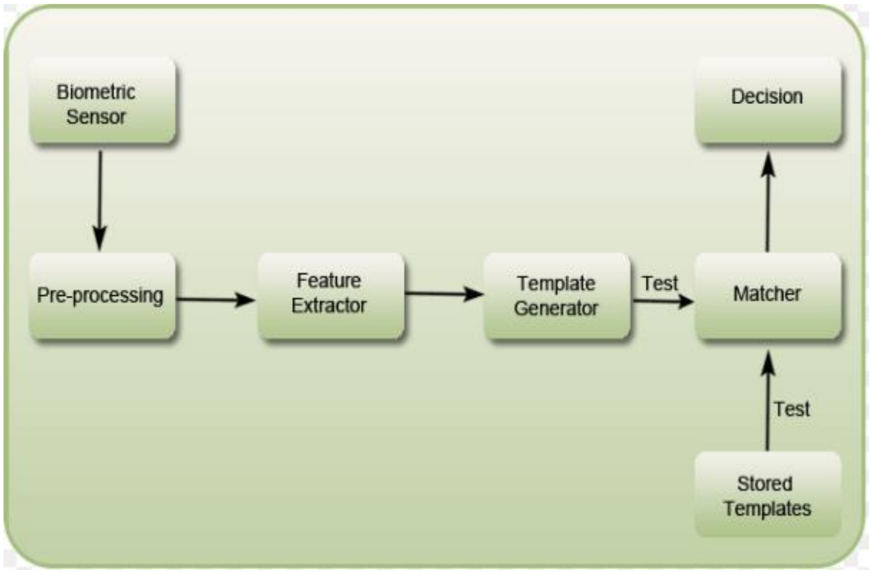

Figure 1: Block diagram of biometric system

III. MOTIVATION

Using biometrics, it is easy to recognize an individual based on the recognition methods. To recognize an individual it has some reasons, they include reducing costs and improving scalability, reducing error rates, improving accuracy, improving convenience and increasing physical safety. To verify a person it is required to have passwords, names, social security numbers, tokens and PINs, so that the person may access its services or benefits. For example ATM card and its corresponding PIN are required to access an automatic teller machine (ATM).

IV. BIOMETRIC MODALITIES

A biometric modality is a method used to verify or recognize a biometric trait. Examples of biometric traits are face, fingerprint, hand geometry, palm print, iris, voice, signature, gait, and keystroke dynamics. The user's biometric features involve both biological and behavioral aspects. Some common biometric modalities are summarized here.

Face recognition method requires a digital camera to develop a facial image for authentication. It analyzes facial characteristics. The casino industry is working on this technology for quick detection by security personnel to create a facial database of scam artists.

In **fingerprint** recognition method, there are various approaches to fingerprint verification. It is found on a fingertip and looks like a pattern on a fingerprint. Some approaches are matching minutiae, others use straight pattern- matching devices, and moirefringe patterns and ultrasonics. Some verification approaches are used to detect when a live finger is presented and some cannot.

For in-house systems fingerprint verification may be a good choice. Fingerprint verification can provide adequate explanation and training to users and it operates in a controlled environment. The workstation access applications are based on fingerprints due to low cost, small size and ease of integration.

Hand Geometry recognition method used to analyze and measure the shape of the hand. Biometric system is easy to use and provides good performance characteristics. Biometrics is suitable where there are more users available and users can access the system infrequently. In this hand geometry recognition method, accuracy is very high if there is desired and flexible performance tuning and configuration. Hand geometry are available in various scenarios for example time and attendance recording, these are proved in organizations. Hand geometry is the first step in every biometric project due to ease of integration into other processes and systems and coupled with ease of use.

In **Iris** recognition method, it has colored ring of tissue that surrounds the pupil to analyze features of iris images. Iris scanning has higher potential than the average template matching performance. For identification phase, Iris recognition method is one of the few devices that work well and it works with glasses in place. The disadvantages of iris scanning devices are ease of use and system integration.

Retina recognition method used to analyze the layer of blood vessels located at the back of the eye. This technique uses a low- intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning requires the user to look into a receptacle and focus on a given point. Retinal scanning can be accurate. If you wear glasses, then retinal scanning is not particularly convenient or these are concerned about having close contact with the reading device. This technique works well even though it is not accepted by all users.

Signature verification method analyzes how a user signs her/his name. Some of the signing features are speed, velocity, and pressure. These are the finished signature’s static shape and very important. Signature verification is different from other biometrics because it enjoys a synergy with existing processes but other biometrics does not.

Voice authentication is based on voice to print authentication that is it converts voice into text but then it is not based on voice recognition. Voice biometrics does not require any hardware and it has the most potential for growth. And most of the computer systems contain a microphone. Voice Biometrics has some limitations they are poor quality and ambient noise can affect verification. Voice recognition is not user friendly because enrollment phase is more complicated compared to other biometrics. Therefore voice authentication method should require improvement.

Palm Prints uses the combination of some of the features of fingerprints and hand geometry. Human palms are larger like fingerprints and it contains ridges and valleys. Palm prints are mainly used in the forensic community like fingerprints. And also palm prints can often be found at crime scenes.

Gait recognition method includes how a person walks, and human recognition is based on the distance and period of time. Gait recognition systems are used to detect the human spatio temporal attributes and it is based on image processing. Some of the factors of gait are includes choice of footwear, the walking surface, and clothing. The development stage is used in gait recognition systems.

V. BIOMETRICS COMPARISON

There are various numbers of pros and cons for every biometric system. The main aim of biometrics is to change the existing password. Biometrics uses both biological and physiological features to identify a person. Biometrics has some of the features which include iris patterns, retina design, facial geometry, fingerprints, voice recognition and hand recognition and so on.

The following seven factors are:

- Universality
- Uniqueness
- Permanence
- Measurability
- Performance
- Acceptability
- Circumvention

In Universality, using biometric trait every individual should access the application. In Uniqueness, for every person the given biometric trait is different from other person. In permanence, for a given matching algorithm, biometric trait for a person is invariant over time. The biometric trait which changes significantly is not a good biometric. In measurability, the biometric trait uses suitable devices, these devices should be able to acquire and digitize the trait for every individual and it is inconvenience to the biometric trait. The biometrics system uses acquired raw data to process and to extract features from the biometric trait. In performance, biometrics system should have the higher accuracy to meet the requirements of the application and to achieve this accuracy it requires recognition accuracy and the resources are required to achieve the accuracy. In acceptability, every individual should have biometric trait in the system and these individuals will use application to present their biometric trait to the system in the large population. In circumvention, using biometrics it is easy to imitate the artifacts using biometric traits for example, mimicry can be used for behavioral characteristics and for physiological characteristics fake fingers are used to imitate the biometric trait of an every person. Security should be very important, to conform the needs of the application.

VI. UNIMODAL AND MULTIMODAL BIOMETRICS

For identification and verification features, biometric uses a single biometric trait of the person is referred as unimodal biometrics. Biometrics which uses more than two biometric traits of the individual to identify a person is called as multimodal biometrics. The recognition rate can be improved by using multimodal biometrics. Compared to unimodal biometrics, multimodal biometrics is most widely used in the organizations.

VII. LIMITATIONS OF UNIMODAL BIOMETRIC SYSTEMS

Biometrics is used in many applications, some of the main applications are border control and voter id issuance. In unimodal biometrics, theoretically it might be very proficient but in reality it has various numbers of challenges when enrolling large number of people. The unimodal systems are not suitable for all applications, this is the major issue with the unimodal biometrics. Therefore multimodal biometrics is used to overcome the limits of unimodal biometrics.

Limits of unimodal biometrics are follows:

The biometric trait uses susceptibility to remove noisy or bad data. The biometric technology uses the captured biometric data. And due to imperfect acquisition conditions the biometric data might be distorted. By using facial recognition method the limitations can be seen in applications.

With the illumination conditions and facial expressions using these, facial images might affect the quality of the facial features. Example of fingerprint recognition method is that it leads to false database matching because the scanner is not able to read fingerprints clearly. An imposter leads to falsely accepted and enrolled person leads to incorrectly rejected. For elderly and young children, fingerprint images are not able to capture properly due to faded fingerprints or underdeveloped fingerprints ridges. And for groups of population it is not compatible.

Unimodal system is susceptible to inter class similarities for large population. For identical twins facial recognition method may not work correctly. Inaccurate matching is the major issue in the recognition method for identical twins, so camera cannot distinguish between the two subjects. By using unimodal biometrics, the data can be forged or imitated due to spoof attacks. Using rubber fingerprints person information can be easily spoofed and it is possible in the fingerprint recognition systems.

VIII. MULTIBIOMETRICS

Multibiometrics uses two or more biometric traits. By using facial images, fingerprints, iris scanning, hand geometry, voice recognition methods and so on, they can identify a individual person. To measure two or more biometric characteristics, biometric systems take input from single or multiple sensors. Example of multibiometrics is system that combines face and iris characteristics for biometric identification. In order to improve the recognition rate, multibiometrics combines the two or more biometric modalities. Unimodal biometrics does not provide the desire performance. So the best approach to improve accuracy and performance is to use is multibiometrics.

Multibiometrics has several meanings as shown here:

- Multisensors
- Multiple algorithms
- Multiple instances
- Multiple samples
- Multimodal

In multisensors, single biometric trait is used but then to capture the biometric data, multiple sensors are used. For example, to capture different angles on a face multiple cameras are used in the facial recognition system. In multiple algorithms, using different algorithms captured data are processed. For example, by using minutiae and texture fingerprint images are processed. In this method the hardware costs and sensors are saved but then complexity is increased. In multiple instances, for the same modality multiple instances are used in the biometrics. For example, instead of using one fingerprint image multiple fingerprint images may be matched like irises of both eyes. In multisamples, for the same biometric trait multiple samples are acquired. For example, different portions of the fingerprint, it takes multiple images of this fingerprint and multiple angles of face are captured for the fingerprint biometrics. In multimodal, data can be combined by using different modalities, for example face and fingerprint or iris and voice. This biometrics used to capture and process each modality by using both hardware and software systems.

IX. FUSION LEVELS IN MULTIBIOMETRICS

In multibiometrics, two or more biometric trait is used in biometric systems and also decision channels used more than one. Biometric fusion is defined as its aim is to design a procedure, which combines classification outcome from each biometric channel. To decrease the weakness of individual measurements and to enhance the strengths using different biometric attributes, biometric fusion is used widely in the industry.

In biometrics system, implementations of multibiometrics can be done by using levels of fusion. To address number of issues in the biometrics, fusion is used. Some of the issues are robustness, applicability, accuracy, efficiency and universality. To increase robustness of the multibiometrics, various levels of fusion are used for fusing the biometrics traits. Four types of fusions are available they are as follows: sensor level, feature level, matching score level and decision level. The block diagram of fusion levels in a multibiometrics as shown in figure 2.

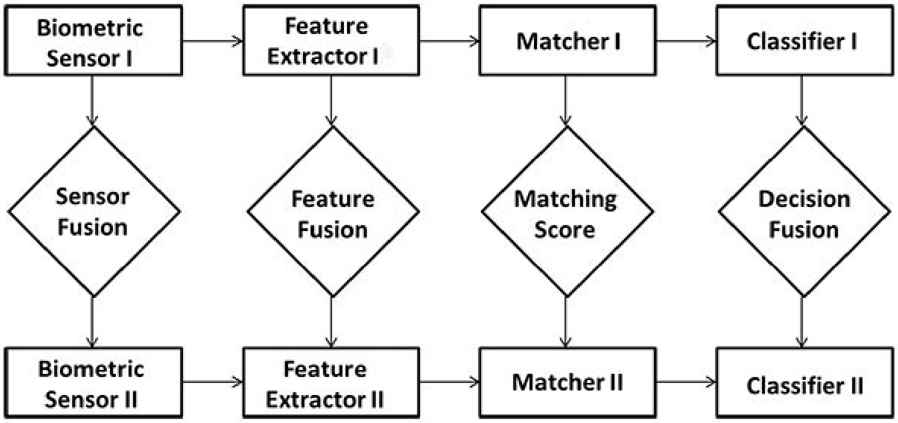

Figure 2: Multibiometrics Fusion levels

A. Fusion using sensor level

Merged biometric trait is formed by using different sensors. For example fingerprint scanner, iris scanner and video camera etc. Fusing of biometrics traits is done by using different sensors. And these biometrics traits are processed.

B. Fusion using Feature level

Signals are processed first which are coming from different biometric traits in the feature level. And later from each biometric trait, separately feature vectors are extracted. In feature level fusion, signals coming from different biometric channels are first processed after which the feature vectors are extracted separately from each biometric trait. The fusion algorithms are used to form composite feature vector by combining feature vectors and later classifications are applied for feature vectors. To select useful features, reduction techniques are used in feature level. Compared to matching score method, feature level contains richer information of biometrics and therefore good recognition results are obtained from feature level fusion. And also when features of different biometric traits are compatible, feature level provides more accuracy.

C. Fusion using Matching score level

Instead of combining feature vectors, they are processed separately in the biometrics. Then matching score for each individual biometric trait is obtained and on the basis of accuracy of biometrics trait, composite matching score is found by fusing matching level. And later classifications are used. To combine match scores, number of techniques is used such as mean fusion, highest rank, logistic regression etc. By using different traits, normalization of scores are acquired which is the important benefit of this fusion. To achieve this normalization of match scores, some of the techniques used are z-score, piecewise linear, min-max etc. Less complexity is obtained from matching score level compared to other fusions and therefore this level of fusion is used widely.

E. Fusion using Decision level

Separately pre-classification of each biometric trait is done first in the decision level. In the biometrics, individual biometric trait is captured first and extraction of features is done from the captured trait. Classification of traits is done as either accepts or rejects on the basis of extracted features. By combining the outputs of different traits, final classification of biometrics is done.

X. PREVIOUS WORK

Sameer P Patil et al., [1] proposes that for many business processes the reliable personal recognition is critical. Based on behavioral and physiological characteristics, biometrics used to refer to automatic recognition of a person. Many biometric and non biometric components are used to provide reliable personal recognition. Biometrics has lot of limitations on security of a system. The main two things that security of a system depends on requirements of an application and cost benefit analysis.

Sameer P Patil et al., [2] proposes an iris and fingerprint biometric traits for user verification system. Two different types of fusion levels are used and compared, they are decision level and score level fusion. The methods used for iris recognition, to extract region of interest are less complex. Better results are obtained from individual modalities. And iris and fingerprint features are fused to increase the recognition accuracy of the system by using fusion levels.

Anil Jain et al., [3] proposes online fingerprint verification for the design and implementation of biometrics. It operates in two stages. First stage is minutia extraction and second stage is minutia matching. Minutia extraction method is much faster and more accurate. An alignment based elastic matching algorithm is developed for minutia matching algorithm. It has the capability of finding correspondences between input minutiae and the stored template. And also it has the ability to compensate the nonlinear deformations and inexact pose transformations between fingerprints. In this system, the verification accuracy is 99% over a 15% of reject rate. By using inkless scanners, it has captured two sets of fingerprint images and tested on biometrics.

Anil Jain et al., [4] proposes by using fingerprints for automatic identity authentication system. It uses an alignment-based elastic matching algorithm. It is capable of finding the correspondences between minutiae without resorting to an exhaustive search. The biometrics achieves an excellent performance. The reason is by using different fingerprints, it has the ability to compensate for the nonlinear deformations and inexact transformations. The advantages of biometrics in this system are response time and accuracy.

Vincenzo Cont et al., [5] proposes an system which has capacity to reject low-quality items that is for online biometric authentication system. Some of the databases are FVC databases, CASIA, and BATH are used to contain images with different quality. Those images includes low, medium, high quality biometric acquisitions. And also they includes partial and corrupted images. Due to these reasons biometrics do not achieves better results. A unified biometric descriptor is used and it is working on a template-level fusion algorithm. Therefore matching algorithm is able to process fingerprint-codified templates, iris-codified templates, and iris and fingerprint-fused templates.

S. Liu et al., [6] proposes a user access, e-commerce and other security applications by using secure authentication method. With the help of physically and behavioral characteristics biometrics are used to identify a person, for that reason biometrics is used. For examples fingerprint, hand or palm geometry, and retina, iris, or facial, signature, voice, keystroke, pattern, and gait. Here, signature and voice biometrics traits are used to implement the proposed work.

H. B. Kekre et al., [7] proposes biometrics technology for personal authentication. For biometrics system a lot research is going on in this technology. By using sensors, human traits are captured with the help of these technologies. Here mainly discussing about an biometrics domain research for application development, which is focused on interfacing sensor devices. They are used to capture data in usable form. The component object model and .net platform are used in the biometrics system. they are used to interface sensors in the biometrics. There are three components authentication, authorization and accountability for security.

Gunjan Jiwnani and Nisheeth Saxena [8] proposes multibiometrics identification technology by using fuzzy method. In proposing model, it is using two biometric traits fingerprint and iris and after performing the processing individually. Fuzzy technique is applied and finally takes decision that the authentication is very high or low. Biometric systems are used for authentication due to limitations of traditional systems like using PIN, PASSWORD etc. Single biometric trait also has some limitations so to overcome these limitations, biometric systems uses multi biometric authentication which gives result with more accuracy but also requires more storage as compared to single biometric.

Piyush G. Kale, Khandelwal C.S. [9] proposes PCA technique for IRIS and Finger print biometrics. For proposed model, multibiometrics fuses PCA minutia extraction and Weighted LBP feature extraction. The results from these extractions are applied on different biometric traits. To identify a person the IRIS and Fingerprint are used in the proposed system. To compare performance and accuracy different recognition methods are used. Examples of classifiers are SVM & ANN. These are used for matching.

H B Kekre, V A Bharadi et al., [10] proposes face and iris biometrics for a combination of unimodal and multi-algorithmic systems. By using multilevel decomposition algorithm, face features are extracted, with the help of Kekre's wavelet. And by using 1 D transform of row and column mean, iris features are extracted. Kekre's wavelet based texture features and Kekre's Fast Code book Generation (KFCG) & Kekre's Median Codebook Generation (KMCG) algorithms are used for VQ codebooks.

XI. CONCLUSION

Here, general biometrics, motivation of using biometric system, biometric recognition methods, and numerous issues of unimodal biometrics has been discussed. A biometric system which uses single biometric trait to identify a person it is referred to as unimodal biometrics. Using unimodal biometrics it is very difficult to achieve performance. So in order to improve performance of the biometrics, multimodal biometrics is used. An overview of applications of multibiometrics and its different fusion levels are discussed. In today's applications, higher performance and level of security can be improved due to multibiometrics.

REFERENCES

[1] Sameer P Patile, Tushar N Raka, Shreyas O Sarode, "Multimodal Biometric Identification System: Fusion of Iris and Fingerprint", *International Journal of Intelligent Information Technology Application (IJIITA),* Vol. 2, No.6, ISSN 1999-2459 (print), December,pp. 279-285, 2014.

[2] Sameer P Patil, Tushar N Raka, "Multimodal Biometric Identification System: Fusion of Iris and Fingerprint".

[3] Anil Jain, Lin Hong, "On-line Fingerprint Verification" *International Journal of Advanced Research in Computer Science and Technology* , vol. 2, Issue Special 1, Jan-March 2012.

[4] Anil Jain , Lin Hong , Sharath Pankanti, "An Identity Authentication System Using Fingerprints".

[5] Vincenzo Conti, Carmelo Militello, Filippo Sorbello, "A frequency-based Approach for features fusion in fingerprint and iris multimodal biometric identitification systems" *International Journal of Ophthalmol*, vol. 8, No.1, Feb 2013.

[6] S. Liu, M. Silverman, "A practical guide to biometric security technology", IT Professional, Vol. 3, No. 1., pp. 27-32, Aug 2002.

[7] H. B. Kekre, V. A. Bharadi, "Using Component Object Model for Interfacing Biometric Sensors to Capture Multidimensional features" , *International Journal of Intelligent Information Technology Application (IJIITA),* Vol. 2, No.6, ISSN 1999-2459 (print), December, pp. 279-285, 2009.

[8] Gunjan Jiwnani, Mr. Nisheeth Saxena, " Multimodal Biometric Authentication using Fingerprint and Iris: a Review", *International journal of computer science & Communication Networks,* Vol 5(2), 115-119

[9] Piyush G. Kale, Khandelwal C.S., M.E.(EC), *Department of Electronics & Telecommunication,* "IRIS & Finger Print Recognition Using PCA for Multi Modal Biometric System", *International Conference on Global Trends in Engineering, Technology and Management (ICGTETM-2016)*

[10] H B Kekre, V A Bharadi, V I Singh, V Kaul, B Nemade., " Hybrid Multimodal Biometric Recognition using Kekre's Wavelets, 1D Transforms & Kekre's Vector Quantization Algorithms Based Feature Extraction of Face & Iris" *2nd International Conference and workshop on Emerging Trends in Technology(ICWET-2011)*

[11] Kamel Aizi, Mohamed Ouslim, Ahmed Sabri., "Remote Multimodal Biometric Identification Based on the Fusion of the Iris and the Fingerprint", *International Conference on Information Science and control Engineering (ICISCE)*, pp. 1-5, 2015

[12] B. C. Kovoor, M.H. Supriya and K. Poulose Jac, "A prototype for a multimodal biometric security system based on face and audio signatures", *International Journal of computer Science and Communication* vol. 2, no. 1, pp. 143-147, January-June 2011.

[13] Zatin Singhal, Preeti Gupta and Kavitha Garg, "Biometric recognition Personal identification technique", *Ijcem International Journal of Computational Engineering & Management,* vol. 15, Issue 3, May 2012.

[14] J.A. Unar, Woo Chaw Seng and Almas Abbasi, "A review of biometric technology along with trends and prospects," Pattern recognition, accepted manuscript.

[15] A. H. Mir, S. Rubab and Z. A. Jhat, "Biometrics verification: a literature survey," *International Journal of Computing and Ict research,* vol. 5, no 2, December 2011.

[16] Rohit Katiyar, Vinay Kumar Pathak and K. V. Arya, " A study on existing gait biometrics approaches and challenges," *Ijcsi International Journal of Computer Science issues,* vol. 10, issue 1, no 1, January 2013.

[17] M.J. Sudhamani, M.K. Venkatesha, K.R. Radhika, "Revisiting Feature level and Score level Fusion Techniques in Multimodal Biometrics System," *Proceedings of International Conference on Multimedia Computing and Systems (ICMCS),* pp. 881-885, 2012.

[18] Y. Tong, F. W. Wheeler, X. Liu, "Improving Biometric Identification through Quality based Face and Fingerprint Biometric Fusion," *Proceedings of IEEE Computer Society Conference Vision and Pattern Recognition Workshops,* pp. 53-60, 2010.

[19] A. Kumar, Y. Zhou, "Human Identification Using Finger Images," *IEEE Transactions on Image Processing*, vol. 21, n. 4, pp. 2228-2244 2012.