Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. 1, Issue 5 – December 2021, Pages: 8-14

Fingerprint and Lip Images for Multibiometric Recognition and Verification

Mr. K. Gerard Joe Nigel
Assistant Professor
Karunya Institute of Technology and Sciences
Email: gerardnigel@karunya.edu

Abstract: Nowadays, biometric authentication is a great approach to ensure security. It has now been established that each human has a unique biometric trait such as a fingerprint, iris, lips, palm, face, and voice. Individuals are identified and their identities are verified via biometric recognition. This study employs two biometric modalities, namely lip and fingerprint, to increase identification accuracy. To solve the shadow, beard, and rotation issues in lip identification, five different mouth corners are recognised. Minutiae score matching is employed in fingerprint identification, and fingerprint verification is done by extracting and matching minutiae. In this multi-biometric recognition, a support vector machine is used for classification. When lip biometric is used with fingerprint biometric, the recognition results improve. We demonstrate that our suggested approaches are suitable for a wide range of recognition applications in security and forensics-oriented computer vision, such as biometrics, object identification, and content-based picture retrieval.

Keywords— Biometric, Lip recognition, Fingerprint recognition, Multi-biometric, Fusion, SVM, Minutiae.

1. INTRODUCTION (*Heading 1*)

Biometrics is derived from the Greek words "bio" (life) and "Metrics" (measurement) (to measure). Biometrics uses a person's physiological or behavioural traits to verify their identification [1]. In general, a biometric system gathers a person's biometric data, extracts the necessary feature set from the data, compares this feature set to the feature set(s) already recorded in the database, and authenticates or denies the individual depending on the outcome of this comparison. The success of a biometric system is determined first by the right selection of biometric data, followed by the methodologies used to go from raw data to a conclusion. The specified application domain of the system determines which biometric data will be utilised.

Biometric data should have the following characteristics: I universality – every person should have this characteristic, (ii) uniqueness – no two people should have the same characteristic, (iii) permanence – the characteristic should remain constant over time, and (iv) collectability – the characteristic can be measured quantitatively. (vi) acceptance – reflects people's readiness to supply this biometric feature, (v) performance – relates to the accuracy of identification based on resource needs and environmental conditions, (vii) circumvention – refers to how simple it is to deceive the system using deceptive methods.

A biometric system is simply a pattern recognition system that identifies a person by assessing the authenticity of the individual's physiological and behavioural traits. Physiological biometrics, also known as physical or static biometrics, is based on data obtained by measuring a portion of an individual's body. Fingerprint recognition, Iris scan, Retina scan, Hand Geometry; Palm print, Face recognition, DNA and Vascular Pattern Recognition are some of the features included. One of the oldest technologies is fingerprint recognition. Behavioural biometrics, also known as dynamic biometrics, is based on data collected from measurements of an individual's activity, using time as a metric. The action is measured in three parts: beginning, middle, and finish. Signature, keystroke, handwriting, voice recognition, and gait are all included. Soft biometrics is a human trait that provides information about the person but lacks the uniqueness and permanence needed to distinguish any two people. Scars, markings, tattoos, and the colour of skin and hair colour are examples of soft biometrics [2]. Insecure communication systems, reliable authentication is critical. Passwords (knowledge-based security) and smartcards (token-based security) have traditionally been employed as the initial step in proving identification in the system. However, security may be compromised since dynamic passwords are readily revealed and guessed via social engineering or dictionary attacks. Token-based authentication may be able to compensate for the knowledge-based authentication's limitations.

It is, however, unreliable and readily stolen. When passwords and smartcards are shared or stolen, a type of individual authentication based on physiological or behavioural qualities associated with the person overcomes the problems of passwords and smartcards, although it is well known that single biometric data is always noisy and distorted. Multibiometrics uses numerous biometric modalities to overcome the limitations of unimodal biometrics. Due to the

inclusion of many reasonably independent pieces of evidence, these systems are considered more dependable. Multibiometric systems combat non-universality and offer anti-spoofing protection by making it impossible for an attacker to spoof many biometric attributes of a valid user simultaneously. When building a multibiometric system, many issues need to be considered. These factors include the quantity and kind of biometric characteristics used and the level in the biometric system at which information from several traits should be combined.
Because a single biometric system is insufficient for authentication and identification, some of the limitations imposed by unimodal biometric systems can be overcome by incorporating multiple sources of identity information [3], which allows the integration of two or more types of biometric systems. Excellent performance and security are achieved when many modalities are used in user verification and identification. The remainder of the paper is broken into the following sections. In Section II, we explain previous work, and in Section III, we describe meta-recognition. Finally, in Section IV, we present and comment on our findings, and in Section V, we finish this study with a conclusion and future work.

2. **PRIOR WORK**

Fusion may occur at two levels in a multibiometric system: fusion before matching (sensor and feature levels) and fusion after matching (sensor and feature levels) (match score, rank, and decision levels). Because the quantity of information accessible to the fusion module reduces as we go from the sensor to the decision level, fusion is generally more efficient at the earlier stages, such as before matching.

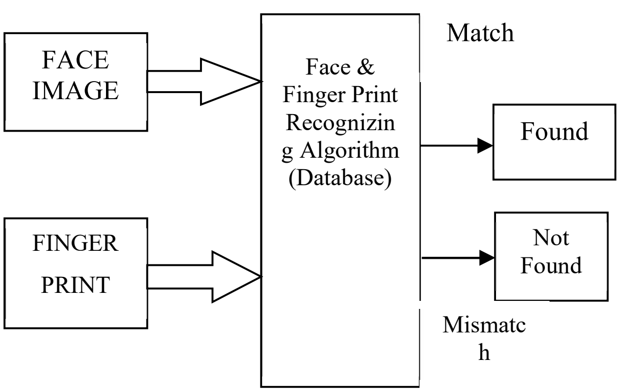

Fig. 1 Prior architecture diagram

However, fusion at the decision, score, or rank levels is the only realistic option in most commercial biometric systems. Compared to decision level fusion, rank level fusion gives additional insight into the matcher's decision-making process. At the same time, it avoids the normalisation issue that score level fusion techniques are prone to.

A. Face Biometric

Zhao et al. surveyed facial recognition methods (2003). Face recognition algorithms may be classified into two classes depending on the face representation that they use [4].
Appearance-based: employs holistic texture elements to apply to the whole face or particular areas of a face picture; Geometric face features (mouth, eyes, brows, cheeks, etc.) and geometric connections between them are used in feature-based modelling.

B. Fingerprint Biometric

Because of their practicality, uniqueness, permanence, accuracy, dependability, and acceptance, fingerprints have been extensively employed in everyday life for more than a century [5]. The fingerprint matching method determines if two sets of fingerprint ridge detail are from the same finger. There are a variety of algorithms that can match fingerprints in various ways. Some approaches compare minutiae points between the two photos, while others seek similarities in the fingerprint's larger structure and suggest a minutiae matching method for fingerprint matching.

3. META-RECOGNITION

Meta-purpose recognition's is to automatically forecast whether a match will be a success or a failure. Statistical meta-recognition provides various advantages over machine learning-based algorithms, including the lack of training data, ease of implementation, and the ability to use the CDF of the selected EVT distribution for robust score normalisation. However, if we can train machine learning classifiers with the proper features, we can get more accurate results for prediction than we can with pure statistics. In the theoretical meta-recognition paradigm, the judgments produced by machine learning classifiers are "predictions." We created unique techniques to integrate features for learning calculated over raw recognition scores and the judgments made by separate classifiers as part of our research in this publication [6].

A. Features from Scores

Meta-purpose recognition is forecast if a match will be a success or a failure in some automated way.

Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. 1, Issue 5 – December 2021, Pages: 8-14

Statistical meta-recognition provides various advantages over machine learning-based algorithms, including the lack of a requirement for training data, ease of implementation, and the ability to use the CDF of the selected EVT distribution for robust score normalisation. However, we can get more accurate predictions than pure statistics using the correct mix of information to train machine learning classifiers. In the theoretical meta-recognition framework, the judgments produced by machine learning classifiers are called "predictions." We created unique approaches to integrate features for learning calculated over raw recognition scores and individual classifier judgments as part of the research presented in this work [6].

B. Building and Using Classifiers

To develop a meta-recognition classifier, we must first gather the required training data. It is critical to collect the same number of samples for positive match instances (correct rank-1 recognition) and negative match instances (incorrect rank-1 recognition) from sequences of scores from the recognition algorithm to build a classifier with balanced training and testing data. We utilise these scores as the source data for the characteristics specified in Features from Scores. The generated feature vectors are labelled (positive or negative) and may be fed into any machine learning algorithm as training input.

We utilised support vector machines (SVM) as an example in this study. However, any supervised learning technique might be applied (indeed, our group has already shown boosting and neural networks approach to work for post recognition score analysis). The fact that SVMs are well-known, do not rely on the dimensionality of the input space, employ structural risk reduction, and enable quick testing (sub-linear time) of an input sample are all factors that influenced our decision. In Meta-Recognition, we assess the possibilities of various supervised learning methodologies.

We may train an SVM classifier using feature vectors to discover the underlying nature of the score distributions. In practice, a radial basis function kernel produces the best results for this kind of feature data obtained from scores. Linear and polynomial kernels were also explored. However, the radial basis function kernel produced the most accurate results.

We don't need to focus on anything. Any probe/gallery combination is allowed if the training and validation data do not overlap. We can handle dynamic galleries because of our freedom. While the feature computation in features from scores normalises the underlying data, it does not generically rearticulate the scores. Existing techniques have tended to train a classifier based only on the scores from the recognition algorithm or sensor under consideration. We may construct a feature vector from the obtained scores during live recognition and then use the machine learning-based meta-recognition approach to generate our forecast.

4. PROPOSED SYSTEM

Lip recognition and fingerprint recognition are two biometrics that may be employed in the suggested system for recognition. It isn't easy to recognise someone's identity just by their lips. Rapid box filtering is provided in the first step of the proposed system to create a noise-free source with high processing efficiency. Following that, the suggested method detects five different mouth corners while overcoming shadow, beard, and rotation issues. Using the support vector machine, two geometric ratios and ten parabolic-related factors extract features for further recognition.

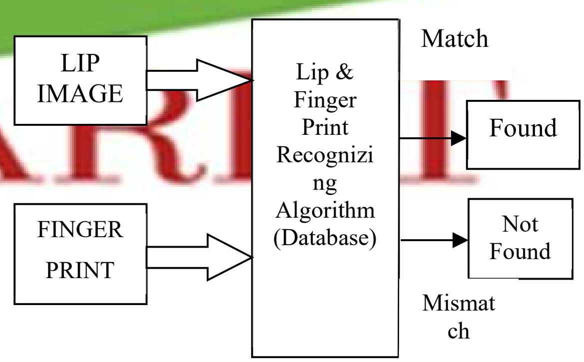

Fig. 2 Proposed architecture diagram

A. Fingerprint Biometrics

The characteristic pattern of one finger is referred to as a fingerprint. Each fingerprint is thought to be unique based on substantial evidence. Each person's fingerprints have a lasting distinctiveness to them. For a long time, fingerprints have been utilised for identification and forensic inquiry. Many ridges and furrows make up a fingerprint. In each tiny local window, these ridges and furrows have many characteristics, such as parallelism and average width. Fingerprints are differentiated not by their ridges and furrows but by Minutia, aberrant places on the ridges, as shown by extensive fingerprint identification studies. The two most important and often used minutia kinds documented in the literature are termination and bifurcation [7]. Termination refers to the immediate terminus, while bifurcation refers to the point on the ridge from where two branches emerge.

Fig. 3 Fingerprint Image

This project aims to create a full fingerprint verification system that extracts and matches minutiae. Pre-processing in image enhancement and binarisation is done to fingerprints before they are examined to ensure effective minutiae extraction in fingerprints of different quality. A minutia extractor and a minutia matcher were built using a combination of approaches. The work employs minutiae marking techniques that consider the triple branch counting and false minutiae elimination methods. For minutia matching, an alignment-based elastic matching method has been devised. This technique can detect the correspondences between the input minutia pattern and the stored template minutia pattern without resorting to exhaustive search. The generated system's performance is then assessed against a database of fingerprints from various persons. Fingerprint acquiring device, minutia extractor, and minutia matcher make up a fingerprint recognition system.

Fig. 4 Features of Finger Print Image

The ridge ending and ridge bifurcation are two minutia matching often utilised for fingerprint identification. We used the Minutia Score Matching approach to project Fingerprint Recognition in this work (FRMSM). The Block Filter is used for fingerprint thinning, which scans the picture at the border to retain image quality and recover minutiae from the thinned image [6].

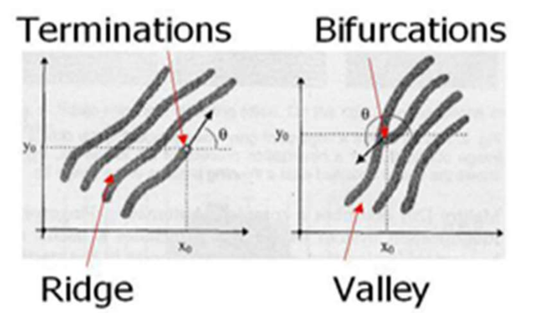

Fig. 5 Minutia Features

B. Lip Biometrics

Five different mouth corners are recognised to solve lip identification's shadow, beard, and rotation difficulties [8]. There are three alternative ways to remove the lip area. The lip area in the first type is formed by the rectangle enclosing the ellipse, which is based directly on the ellipse that approximates the lip shape. It indicates that the lip area's size is not constant and that the region shifts and tilts in response to the lip shape approximation findings. The lip area in the second variation is a horizontal, constant-size square. Its centre is always anchored at the ellipse's centre, and the length of its sides is set and defined by the ellipse's width at the start of the calibration procedure. In the third variation, the ellipse has little impact on the extraction of the lip area.

The square, whose size and location are set and defined at the start of the calibration process, forms the lip area. The square's centre lies in the ellipse's centre, and the length of its sides is half the width of the whole

Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)

Vol. 1, Issue 5 – December 2021, Pages: 8-14

mouth area. When the lip shape approximation technique fails, the third version comes in handy.
Kass et al. initially proposed the active contour model algorithm[9], which deforms a contour to latch onto objects of interest inside an image. Lines, edges, and object boundaries are often used features. An active contour is an image plane collection of n points that are ordered:

V={v1,v2,…,vn}
Vi =(xi, Yi),i=1,2,…n (1)

The points in the contour iteratively approach the boundary of an object through the solution of an energy minimisation problem. For each point in the neighbourhood of vi, an energy term is computed:

Ei = Eint(vi) + Eext(vi) (2)

Point (vi) is an energy function dependent on the shape of the contour, and Next(vi)is an energy function dependent on the image properties, such as the gradient, near point Vi. The internal energy function used herein is defined as follows:

Eint (vi) =CEcon (vi) +bEbal(vi) (3)

CEcon (vi) is the continuity energy that enforces the shape of the contour, and Ebal (Vi) is a balloon force that causes the contour to grow or shrink, c and b provide the relative weighting of the energy terms. The external energy function attracts the deformable contour to interesting features in an image, such as object boundaries. Image gradient and intensity are obvious characteristics to look at.

The external energy function used herein is defined as follows:

Eext (vi) = mEimg (vi) + gEgrad (vi) (4)

Eimg (vi) is an expression that attracts the contour to high or low-intensity regions, and Egrad (vi) is an energy term that moves the contour towards edges. Again, the constants, m and g, are provided to adjust the relative weights of the terms.

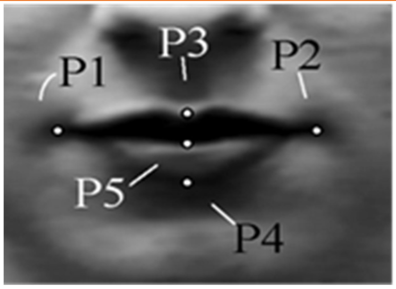

Fig. 6 Five feature points of lips.

C. Levels of Fusion

Different degrees of fusion may be specified based on the information accessible in a given module [10]. The different stages of fusion are divided into two categories by Sanderson and Paliwal: pre-classification or fusion before matching and post-classification or fusion after matching. Because the quantity of information accessible for fusion decreases dramatically after the matcher is triggered, such a classification is required. Because the matches utilised by the separate sources may no longer be applicable, pre-classification fusion methods often need new matching algorithms, posing additional obstacles. Fusion at the sensor (or raw data) and feature levels are used in pre-classification schemes, whereas fusion at the match score, rank and decision levels is used in post-classification schemes.
1. Sensor-level fusion: The richest source of information is raw biometric data (e.g., a facial picture) collected from a person, even though it is likely to be polluted by noise (e.g., non-uniform illumination, background clutter, etc.). Sensor level fusion combines (a) raw data collected from several sensors or (b) many snapshots of a biometric obtained from a single sensor.
2. Feature-level fusion: Feature sets originating from several biometric methods are merged into a single feature set using suitable feature normalisation, transformation, and reduction strategies. The main advantage of feature-level fusion is that it allows for the discovery of associated feature values produced by multiple biometric algorithms and the identification of a key collection of features that may increase recognition accuracy. Feature-level fusion implies the availability of a large quantity of training data since obtaining this feature set often necessitates dimensionality reduction techniques. After consolidating the feature set, the feature sets being fused are often anticipated to exist in comparable vector space to use an appropriate matching approach.
3. Score-level fusion: In score-level fusion, several biometric matchers' match scores are merged to produce a new match score (a scalar) that may then be

utilised by the verification or identification modules to provide an identity decision. Fusion at this level is the most often discussed strategy in the biometric literature, owing to the simplicity with which match scores can be accessed and processed (compared to the raw biometric data or the feature set extracted from the data). There are three types of fusion methods at this level: density-based schemes, transformation-based schemes, and classifier-based schemes.

4. Rank-level fusion: When a biometric system is used to identify a person, the system's output may be considered a ranking of the enrolled identities. In this scenario, the result displays a list of probable matching identities organised by the confidence level. The purpose of rank level fusion techniques is to combine the rankings produced by separate biometric subsystems to arrive at a consensus rank for each identity. Ranks give more information about the matcher's decision-making process than merely the best match's name, but they disclose less information than match scores. However, unlike match scores, the rankings generated by different biometric systems are similar. Consequently, there is no requirement for normalisation, making rank level fusion methods easier to execute than score level fusion procedures.

5. Decision-level fusion: Many commercially available (COTS) biometric matches only provide you access to the final recognition decision. Only decision level fusion is possible when such COTS matches are utilised to form a multibiometric system. "AND" and "OR" rules, majority voting, weighted majority voting, Bayesian decision fusion, the Dempster-Shafer theory of evidence, and behaviour knowledge space are some of the methods presented in the literature for decision level fusion.

Matching scores include enough information to identify real and imposter cases, and they are reasonably inexpensive to generate; hence score level fusion is often used in multimodal biometric systems. Even without knowing each system's underlying feature extraction and matching methods, matching scores for a pre-specified number of people may be calculated given several biometric systems. As a result, employing score level fusion to combine data from several modalities seems to be both viable and practicable. Because the results provided by a biometric system might be either similarity or distance scores, they must be converted into a similar nature [11].

5. EXPERIMENTAL RESULTS

Different degrees of fusion may be set based on the information accessible in a particular module [10]. Sanderson and Paliwal divide fusion into two categories: pre-classification or fusion before matching and post-classification or fusion after matching. Because the quantity of information accessible for fusion rapidly decreases after the matcher is triggered, such a classification is required. Pre-classification fusion systems usually need new matching procedures (since the matters utilised by the separate sources may no longer be appropriate), which adds to the difficulty. Fusion at the sensor (or raw data) and feature levels is part of the pre-classification scheme, whereas fusion at the match score, rank and decision levels is part of the post-classification scheme.

1. Sensor-level fusion: The richest source of information is raw biometric data (e.g., a facial picture) collected from an individual. However, noise is likely tainted by noise (e.g., non-uniform illumination, background clutter, etc.). Sensor level fusion is the process of combining (a) raw data collected from numerous sensors or (b) several snapshots of a biometric captured by a single sensor.

2. Feature-level fusion: Feature sets from several biometric methods are merged into a single feature set using suitable feature normalisation, transformation, and reduction strategies in feature-level fusion. The main advantage of feature-level fusion is that it allows for the discovery of associated feature values produced by multiple biometric algorithms and the identification of a key collection of features that may help enhance recognition accuracy. Feature-level fusion implies the availability of a substantial amount of training data since obtaining this feature set often necessitates dimensionality reduction techniques. After consolidating the feature set, the feature sets being fused are often assumed to exist in similar vector space to use an appropriate matching strategy.

3. Score-level fusion: In score-level fusion, several biometric matchers' match scores are merged to produce a new match score (a scalar) that may be utilised by the verification or identification modules to provide an identity decision. Due to the simplicity of obtaining and processing match results, fusion at this level is the most widely mentioned strategy in the biometric literature (compared to the raw biometric data or the feature set extracted from the data). Density-based schemes, transformation-based schemes, and classifier-based schemes are the three primary kinds of fusion approaches at this level.

4. Rank-level fusion: When a biometric system is used to identify people, the system's output may be considered a ranking of the enrolled identities. This example shows a list of probable matching identities organised by the confidence level. The purpose of rank level fusion techniques is to combine the ranks generated by separate biometric subsystems to provide a consensus rank for each identity. Ranks disclose more information about the matcher's decision-

making process than merely the best match's identity, but they do so at the expense of match scores. The rankings generated by several biometric systems, unlike match scores, are equivalent. Consequently, rank level fusion strategies are easier to execute than score level fusion procedures since no normalisation is required.

5. Decision-level fusion: Many COTS biometric matches only provide you access to the final recognition decision. Only decision level fusion is possible when COTS matches construct a multibiometric system. The Dempster-Shafer theory of evidence, majority voting, weighted majority voting, Bayesian decision fusion, and behaviour knowledge space are some methods presented in the literature for decision level fusion.

Because matching scores provide enough information to identify real from imposter cases and are reasonably straightforward to collect, score level fusion is often favoured in multimodal biometric systems. Even if you don't know each system's underlying feature extraction and matching algorithms, you can calculate matching scores for a pre-specified number of users given a set of biometric systems. As a result, score level fusion seems viable and practical for merging information from individual modalities. Because the results provided by a biometric system might be similarity or distance scores, they must be converted into a similar nature [11].

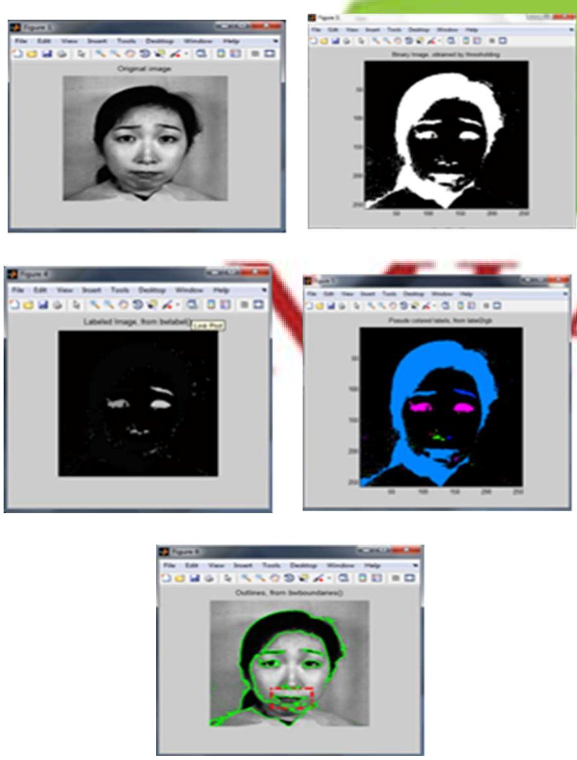

Fig: Images for lip recognition

6. CONCLUSION AND FUTURE WORK

This study implements a multimodal biometric identification system that uses two modalities, namely finger and lip recognition, to authenticate the original picture and may be used for surveillance purposes. Although most biometric systems used in real-world applications are unimodal, meaning they rely on the evidence of a single source of information for authentication, these systems face several challenges, including noise in sensed data, intra-class variations, inter-class similarities, non-universality, and spoof attacks. By using various sources of information for determining identification, some of the restrictions imposed by unimodal biometric systems may be addressed. These systems enable two or more kinds of biometric systems to be combined. High performance is achieved by combining different modalities in user verification and identification.

Recognition is simple with multi-sampling and fusion at the decision level. We may be able to employ more than two biometrics as inputs in the future to increase recognition rates. We are now attempting to improve the recognition rate in an uncontrolled environment to apply it to surveillance applications.

REFERENCES

[1] A.Ross, K.Nandakumar and A.K. Jain, Handbook of Multibiometrics", New York: Springer,2006.

[2] Jain A.K, Dass SC and Nandakumar K, "Soft Biometric Traits for Personal Recognition Syst Proc of International Conference on Biometric Authentication, Hong Kong: 731-738, 2004.

[3] Brunelli, R., and Falavigna, D. "Person Identification Using Multiple Cues", IEEE Trans. on Pattern Analysis and Machine Intelligence (Oct. 1995). IEEE, NY, 955–966.

[4] Nazmeen Bibi Boodoo, "R K Subramanian Robust Multi-biometric Recognition Using ace and Ear Images" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009.

[5] Ravi. J, K. B. Raja, Venugopal. K. R "Fingerprint Recognition using Minutia score Matching" IJEST vol.1(2), 2009.

[6] Walter J. Scheirer, Member, IEEE, Anderson de Rezende Rocha, Member, IEEE, Jonathan Parris, Student Member, IEEE, and Terrance E. Boult, Member, IEEE "Learning for Meta-Recognition."

[7] L. Ravi Kumar, S. Sai Kumar, J. Rajendra Prasad, B. V. Subba Rao, P. Ravi Prakash "Fingerprint Minutia Match Using Bifurcation Technique" S Sai Kumar et al., International Journal of Computer Science & Communication Networks, Vol2(4)

[8] Yun-Fu Liu, Student Member, IEEE, Chao - Yu Lin, and Jing-Ming Guo, Senior Member, IEEE "Impact of the Lips for Biometrics"

[9] Michael Kass, Andrew Witkin, and Demetri Terzopoulos. "Snake: Active contour models," Int. of Computer Vision, 321-331, 1988.

[10] Arun Ross" An Introduction to Multibiometrics "appeared in proc. of 15th European signal processing conference [EUSIPCO], (Poznan, Poland) September 2007

[11] P. D. Garje, Prof. S. S. Agrawal" Multibiometric Identification System Based On Score Level Fusion" IOSR Journal of Electronics and Communication Engineering (IOSRJECE) ISSN: 2278-2834 Volume 2, Issue 6 (Sep-Oct 2012), PP 07-11