Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Concept of Unimodal and Multimodal Biometric System

Komal Sondhi*
CSE & Baddi University
India

Yogesh Bansal
CSE/IT & Baddi University
India

Abstract— A uni-modal biometric systems have a variety of problems such as noisy data, non-universality, spoof attacks and unacceptable error rate. These limitations can be solved by deploying multimodal biometric systems. Multimodal biometric systems utilize two or more individual modalities, like face, iris, retina and fingerprint. Multimodal biometric systems improve the recognition accuracy more than uni-modal methods. In this paper, two uni-modal biometrics, iris and fingerprint are used as multi-biometrics and show using this biometrics has good result with high accuracy. The newly perposed method perfoms best among the studied biometrics.

Keywords— Fingerprint Recognition, Iris Recognition, Minutiae Extraction, Multi-Biometrics, Unimodal Comparison

I. INTRODUCTION

Single biometric systems have limitations like uniqueness, high spoofing rate, high error rate, non-universality and noise. For example in face recognition, it is affected by position, sadness, happiness and the amount of ambient light. It has been recently clear for most researchers that approximately two percent of the population does not have a legible fingerprint and therefore cannot be enrolled into a fingerprint biometrics system [1]. Today, using multiple biometrics is recommended for overcoming these limitations. Using multiple biometric indicators for identifying individuals, known as multimodal biometrics, has been shown to increase accuracy [2] and population coverage, while decreasing vulnerability to spoofing. The important part in multimodal biometrics is the fusion level of various biometric modalities. Four levels are proposed including sensor level, feature extraction, matching score, or decision levels [3]. In this research, decision level fusion is used. This approach has the advantage of utilizing as much information as possible from each biometric modality. Two modalities i.e. fingerprint and iris will be used in this researches. In first sections a brief review for fingerprint and iris acquiring code is provided, and then the combination method of these two modalities and fusion method are introduced.

II. RELATED WORK

A number of studies have been done on multimodal biometrics and these works show that multi- biometric has more advantage than single- biometric. Brunelli and Falavigna [4] used hyperbolic tangent (tanh) for normalization and weighted geometric average for fusion of voice and face biometrics. Hong and Jain [6] proposed an identification system based on face and fingerprint, where fingerprint matching is applied after pruning the database via face matching. Kittler et al. [5] have experimented with several fusion techniques for face and voice biometrics. Ben-Yacoub et al [7] considered several fusion strategies, such as support vector machines, tree classifiers and multi-layer perceptron, for face and voice biometrics. The Bayes classifier is also used in many methods. Ross and Jain [8] combined face, fingerprint and hand geometry biometrics with sum, decision tree and linear discriminant-based methods. The authors report that sum rule outperforms others. Shubhangi and Manohar Bali proposed multimodal biometric system using face and fingerprint and combining ridge based matching for fingerprint and Eigen face [17].

Fingerprint Recognition

Fingerprint is a graphical pattern of ridges and valleys on the surface of human finger. It has uniqueness and permanence characteristics because of that it can be among the most reliable human characteristics that can be used in several ways for personal identification. Due to well understood biological and biometric formation properties, it has been used for personal identification, identification of criminals by various forensic departments around the worlds since centuries. Most automatic systems for fingerprint comparison are based on minutiae matching. Minutiae characteristics are local discontinuities in the fingerprint pattern which represent terminations and bifurcations. A ridge termination is defined as the point where ridges end abruptly. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridge. These two most prominent characteristics ridge termination and ridge bifurcation, define minutiae of fingerprint image. A good quality fingerprint image contains about 40 to 100 minutiae. A fingerprint is the feature pattern of one finger and it is believed that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and recognition. A fingerprint is composed of ridges and furrows which are parallel and have same width.

Fig. 1 A fingerprint image acquired by an Optical Sensor

However, in fingerprint recognition, fingerprints are not distinguished by their ridges and furrows; they are distinguished by Minutia, which are features on the ridges. There is variety of minutia types on fingerprint image as in the below figure but two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge and the other is called bifurcation, which is the point on the ridge from which two branches derive.

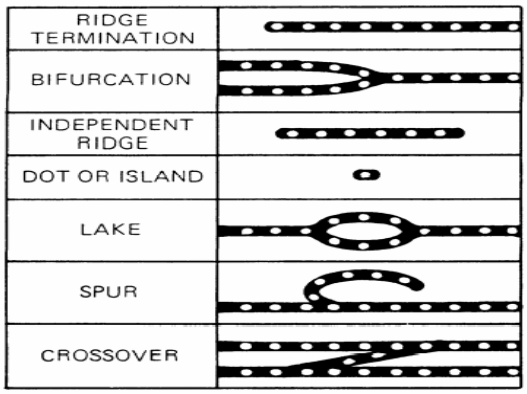
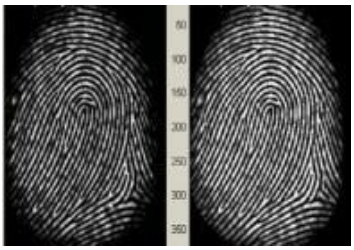


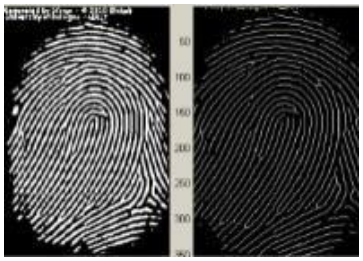
Fig. 1 Variety of minutia types on fingerprint image

Fingerprint identification system has three part that are image acquiring part, minutia extraction part and matching part.

a



b



c

d

If we look closely at our fingers and palm friction ridge skin, we will notice that skin forms a pattern of ridges and valleys, as shown in figure 3. As we can see from figure, these ridges are not continuous lines, they might end or diverge. These points where ridges are not continuous are called minutiae points (features) and today the major of fingerprint recognition algorithms use minutiae features to compare similarity or dissimilarity between two fingerprint templates. Fingerprint ridges are completely created by the seventh month of an individual fetus development, remain the same for whole lifespan [18], and are the last recognizable characteristics to disappear after death [20]. The form of this ridge patterns is randomly and given that even monozygotic twins have different pattern of fingerprints [19]. Two main layers of skin are: epidermis (outer layer) and dermis (inner layer), where ridges belong to epidermis, meanwhile sweat glands, blood vessels (veins), nerves and other cellular structures are inside the dermis. When ridges are injured or other damage of our finger skin, they will recover and retain original with time, thus the property of permanence and uniqueness makes fingerprint leader to the biometric recognition technologies.

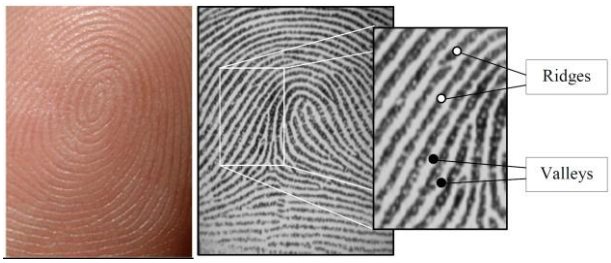


Fig. 3 a) Raw fingerprint image b) Ridge-valley structure of fingerprint image [1]

Iris Recognition

Iris is a circular diaphragm which is located between cornea and lens of the human eye. The function of iris is to control the amount of light entering through the pupil. The average diameter of iris is 12 mm and pupil size can be 10% to 80% of the iris diameter. The iris consists of a number of layers; the lowest layer is the epithelium layer which contains dense color cells and determines the color of iris. Stromal layer consists of blood vessels and the external visible surface is a multi-layered iris that consists of two zones and each zone often differs in color. These two zones are divided by the collarets which make a zigzag pattern. The iris formation happens in the third month of embryonic life and unique patterns are formed during the first year of life. These patterns are random and do not depend on genetic factor and the only characteristic that is dependent on genetics is the pigmentation. Image processing techniques can be employed to convert iris pattern to unique code which can be stored in a database and allows comparisons between templates. The overall process for acquiring and storing iris features with iris images can be listed as follow:

- Image acquisition: take photo of iris with good resolution and quality.
- Segmentation: process the acquiring image for separation of iris from eye image.
- Normalization.
- Feature extraction and feature encoding.
- Storing extracted codes in database and comparing acquiring iris images with codes in database.

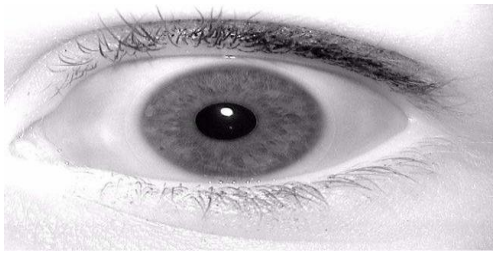


Fig.4 Iris image examples, left eye iris

But in this research, another way is used for segmentation and extraction of iris region. In most previous methods iris edges are found with common edge detection algorithms, but here this algorithm is used:

Taking iris photo an important part in iris recognition and in most images tried to take images with maximum iris region with max opened eyes and no Latency lid on the iris. With using these iris images (CASIA standard database) a rectangle tangent is created to the periphery of the iris surrounding, remove out of rectangle, find an image with maximum part iris and an important advantage with iris in center of image. With having this kind of image first the image size and center pixel can be found with dividing row and column to two and marked this pixel. Certainly the pixel is in the pupil region and its clear pupil is the darker part in eye, so it can move right to the pixel with a high amount of difference intensity and mark it, move left to the pixel with a high amount of difference intensity and mark it and find the center of these points. Do the same and find top and bottom and center of them. Now with these center and peripheral acquired points we can find the real pupil center with center point and maximum distance drawing a pupil circle performing the same task to find the iris region and extract iris from eye image. With Gabor filter features and iris code can be extracted.

After comparing extracted code of a new iris image with codes in database and hamming distance algorithm, the code with minimum difference can be found which can be accepted consequently and save the difference number for an input in our fuzzy logic engine. The human iris is rich in features, can be used to quantitatively to distinguish one eye from another. The iris contains many collagen us fibres, contraction furrows, coronas, crypts, color, serpentine vasculature, striations, freckles, rifts, and pits.

Measuring the patterns of these features and their spatial relationships to each other provides other quantifiable parameters for identification process. The statistical analyses indicated that the Iridian Technologies IRT process uses 240 degrees-of-freedom (DOF), or independent measures of variation to distinguish one iris from another. It allows iris recognition to identify persons with accuracy with a magnitude greater than any other biometric systems. The iris is unique due to the chaotic morphogenesis of that organ. Dr. John Daugman stated that "An advantage the iris shares with fingerprints is the chaotic morphogenesis of its minutiae. The iris texture has chaotic dimension because its details depend on initial conditions in embryonic genetic expression; yet, the limitation of partial genetic penetrance (beyond

expression of form, function, color and general textural quality), ensures that even identical twins have uncorrelated iris minutiae. Thus the uniqueness of every iris, including the pair possessed by one individual, parallels the uniqueness of every fingerprint regardless of whether there is a common genome".

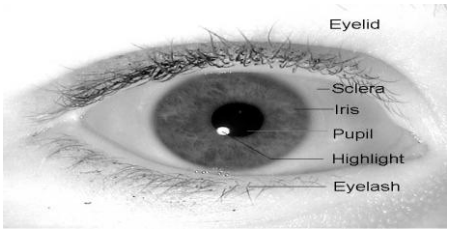


Fig.5 Iris image examples, right eye iris

III. MULTI BIOMETRIC

It is clear that some people have poor quality fingerprints, their face image depends on lighting, their voice can get hoarse due to cold, and also original image of iris projected on a lens can make different biometric authentication systems. All these disadvantages can be overcome with multi-biometric systems which combine the results of two or more biometric characteristics independent from each other. Uni-modal biometric systems perform identification based on single source of biometric information. These systems are affected by many problems like noisy sensor data, non-universality, lack of individuality, lack of invariant representation and susceptibility to circumvention. Because of these problems, the uni-modal biometric systems error rate is quite high which makes them unacceptable for security applications. Some of these problems can be alleviated by using two or more uni-modal biometrics as multi-biometric systems. The architecture of a multi-biometric system depends on the sequence through which each biometrics are acquired and processed. Typically these architectures are either serial or parallel. In the serial architecture, the result of one modality affects the processing of the subsequent modality. In parallel design, different modalities operate independently and their results are combined with appropriate fusion method. The proposed design in this paper is parallel design. There are several paper on different multi-biometric. S.Vasuhi & V. Vaidehi introduce a multimodal biometric system using two well-known biometrics fingerprint and voice [15]. They show using these two single-biometrics together as multi-biometric provides better result. Nageshkumar, M. Mahesh have worked on Palm print and face as multi-biometric [16]. Multi-biometric systems use five different methods for solving single biometric disadvantages:

- **Multi-Sensor**: using two or more sensors for obtaining data from one biometric. (Fingerprint image with two optical and alter sound sensors).
- **Multi-Presentation**: several sensors capturing several similar body parts. (Multi fingerprint image from multi finger of one person).
- **Multi-Instance**: the same sensor capturing several instances of the same body part. (Different position face image).
- **Multi-Algorithm**: the same sensor is used but its input is processed by different algorithm and compares the results.
- **Multi-Modal**: using different sensors for different biometrics and fusion the results. (Like fusion iris and fingerprint code as multi-biometric).

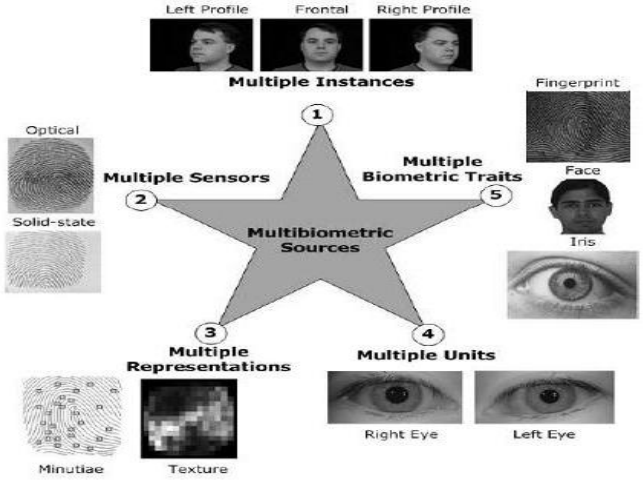


Fig.6 Five different methods for solving single biometric disadvantages

The majority of works done on multi-biometric systems focus on methods that can fusion the single biometric results. For combining two or more uni-modal biometrics and making a multi-biometric system, two or more acceptance results must be combined as fusion. Four possible levels of fusion methods are used for integrating data from two are more biometric systems [9]. These are sensor level, feature extraction level, matching score level and decision level. Sensor level and feature extraction level are called pre-mapping fusion levels but matching score level and decision level are called post-mapping fusion .

A. Levels of Fusion

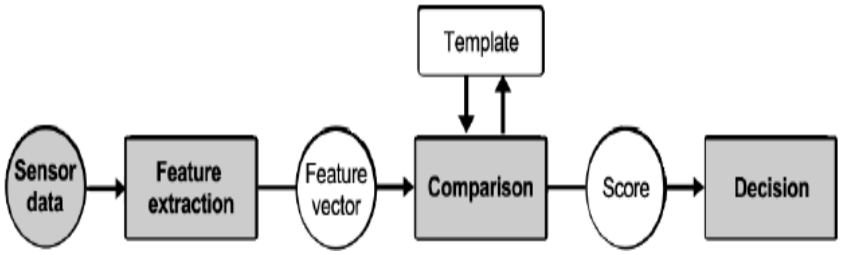


Fig.7 General biometric authentication process flow

In most biometric systems, there are four key processes, as illustrated in figure 7: (1) capturing the biometric trait to be measured in the form of raw data; (2) processing the data extracted into a compressed representation of the trait; (3) comparing the extracted feature set with the reference data, generating a matching score; and (4) using the matching scores to either make an identification decision or to verify a claimed identity.

The use of multiple biometric techniques increases the likelihood of a successful match. Fusion levels can be categorized based on these biometric system components to fuse the biometric information. These fusion levels are described in following sections. According to [16] fusion can be performed at two basic stages:

- **Fusion before comparison**: Integration of information from multiple biometric sources can take place either at the sensor level or at the feature level.
- **Fusion after comparison**: Schemes for integration of information after the comparison stage can be divided into four categories: dynamic classifier selection, fusion at the comparison score level, fusion at the decision level and fusion at the rank level.

B. Fusion at the sensor level. In this level raw data is acquired from sensing the same biometric characteristic with two or more sensors. Sensor level fusion can be done only if the multiple cues of the same biometric are obtained from multiple compatible sensors or multiple instances of the same biometric obtained using single sensor. An example is sensing a speech signal with two sensors. Another example, the face images obtained from several cameras can be combined to form a 3D model of the face. In sensor level fusion, the multiple cues must be compatible.

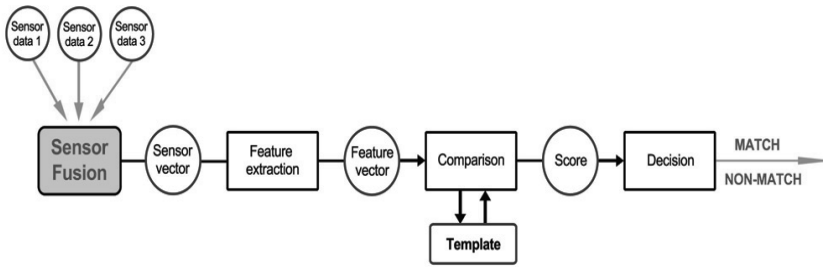


Fig.8 Fusion at sensor level [7]

C. Fusion at the feature extraction level. Fusion at this level can be applied to the extraction of different features from the same modality or different multimodalities. Feature extraction level refers to combining different feature vectors that are obtained from multiple sensors for the same biometric trait or multiple biometric traits. When feature vectors are homogeneous, a single feature vector can be calculated with "and", "or", "xor" or other operations. When the feature vectors are non-homogeneous, we can concatenate them to form a single vector [11] [12].

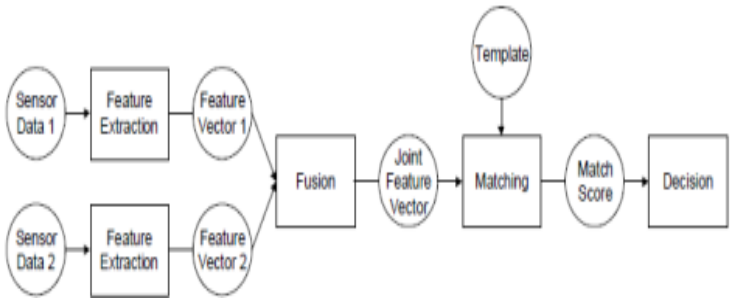


Fig.9 Fusion at the feature extraction Level

.

D. Fusion at matching *score level* At this fusion method there are two approaches for consolidating the scores obtained from different matchers. One of them is to formulate it as a classification problem and the other is as a combination problem. In classification method, a feature vector is constructed by using matching scores output of individual matcher and then classified into two classes: "Accept" and "Reject". In combination method, each individual matching score are used to combine for generating a single scalar score for making the final decision.

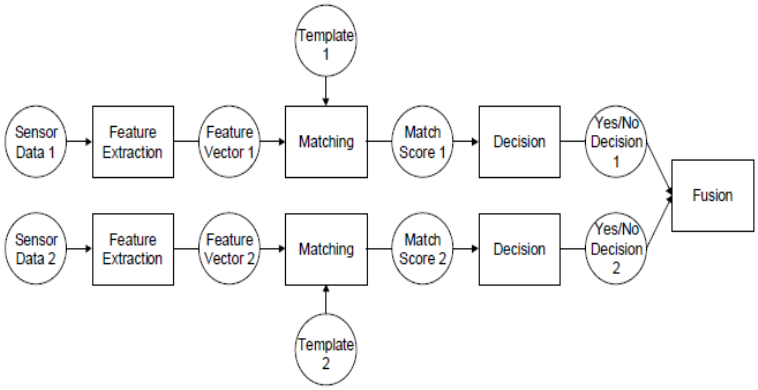


Fig.10 Fusion at matching score level.

E. Fusion at decision level Integration of information at this level can take place when each biometric matcher individually decides on the best match. Methods like majority voting [13] and weighted voting[14] can be used at the final decision. In this approach, we use decision level fusion. At this kind of fusion, a separate decision is taken for each biometric type and then with weighting for each type result, final decision is accepted for final result. Thus, fusion at this level is the least powerful result [10]

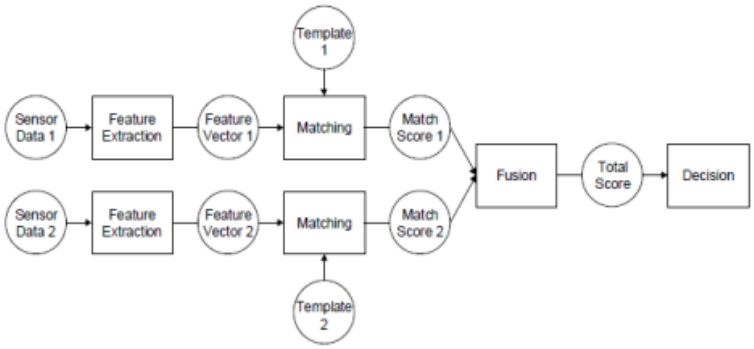


Fig.10 Levels of fusion; FU: fusion module, MM: matching module, DM: decision module.

IV. FUSION

No individual trait can provide 100% accuracy. Thus to overcome the problems faced by individual traits, a novel combination is proposed for the recognition system. The integrated system also provide anti spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. Scores generated from individual traits are combined at matching score level using weighted sum of score technique.

V. EXPERIMENTAL RESULTS

In this section, Single biometric fingerprint is used and find results that is shown in table1. Then iris recognition is used and the result is obtained. Now if multi- biometric is used with fusion fingerprint and iris, better result is accepted.

Table 1 shows differences between two single-biometrics and multi- biometric. In the fingerprint part after converting fingerprint image to binary code, we can compare it with the codes in database with hamming distance and select the code in database with minimum difference. In iris part also do the same and choose the code in database with minimum difference. Fuzzy logic is used for final decision:

TABLE. I
UNI-MODAL

Trait	FAR	FRR	Accuracy
Fingerprint	%3.5	%4	%96
Iris	%5	%5	%97.5

VI. CONCLUSIONS

This research aimed at exploring the use of minutia points and ridge bifurcations to detect spoofing attacks.
Minutiae points and Ridge bifurcations have been detected automatically using a basic detection algorithm. For each image minutiae points and ridge bifurcations along with their extracted locations can be used as a predicting variable. The performance of proposed scheme can be tested by considering a number of image samples. We have shown that intrinsic features, such as minutiae points, obtained directly at the acquisition of friction ridge skin areas can be used as a mechanism to detect spoofing attacks.

Biometric is a unique identity management approach that offers the combination of user convenience, cost effective provisioning and a non- repudiated compliance audit trail for the system operator. After analyzing the feasibility of attacks against fingerprint-based biometric systems, we have shown that the system was able to synthesize templates that guarantee positive identification in a relatively small number of attempts .Even though we proposed several measures to counter such attacks, each has its own limitations, especially for multimodal biometric systems. We need to work on modified attack systems with the aim of decreasing the number of attempts even further.

The paper proposes a biometric personal authentication system using a novel combination of iris and fingerprint. For system deployment the combination is found to be useful as one needs a close up system and other needs contact. One modality is used to overcome the limitations posed by the other. The experimental results show that the accuracy of system would increase on combining the traits.

ACKNOWLEDGMENT

The heading of the Acknowledgment section and the References section must not be numbered.

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

REFERENCES

[1] NIST Report to the United States Congress, "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability", Nov. 13, 2002.

[2] A.K. Jain, R. Bolle, and S. Pankanti, (Eds.), Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999

[3] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2003.

[4] R. Brunelli and D. Falavigna, "Person Identification Using Multiple Cues", IEEE Trans. PAMI, vol. 17, no. 10, pp. 955-966, 1995.

[5] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, "On Combining Classifiers", IEEE Trans. PAMI, vol. 20, no. 3, pp. 226-239, 1998.

[6] L. Hong and A.K. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Trans. PAMI, vol. 20, no. 12, pp. 1295-1307, 1998.

[7] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of Face and Speech Data for Person Identity Verification", IEEE Trans. Neural Networks, vol. 10, no. 5, pp. 1065-1075, 1999.

[8] A. Ross and A.K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, vol. 24, no. 13, pp. 2115-2125, 2003.

[9] S.Pigeon and L. Vandendrope, "Image-based multimodal face authentication," Signal Processing, pp. 59-79. 1997.

[10] A. Ross and A. Jain, "Multimodal biometrics: an overview," Proceedings of the 12th European Signal Processing Conference (EUSIPCO), (Vienna, Austria), pp, 1221-1224, 2004.

[11] A. Kumar, D. C. M. Wong, H. C. Shen, and A. K. Jain. Personal Varification Using Palmprint and Hand Geometric Biometric. In Proceedings of Fourth International Conference on Audio and Video- Based Biometric Person Authentication (AVBPA), pages 669-678, Guiledford, U.K., June 2003.

[12] A.Ross and R. Govindarajan. Feature Level Fusion Using Hand and Face Biometrics. In Proceeding of SPIE Conference on Biometrics Tecnology for Human Identification, volume 5779, pages 196-204, Florida, U.S.A., March 2005.

[13] L.Lam and C. Y. Suen. Application of Majority Voting to Pattern Recognition: An Analysis of its Behavior and Performance. IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans, 27(5):553-568, 1997.

[14] L. Xu, A. Krzyzak, and C.Y.Suen. Methods for Combining Multiple Classifiers and their Applications to Handwriting Recognition. IEEE Transactions on Systems, Man, and Cybernetics, 22(30:418-435,1992.

[15] S.Vasuhi. V.Vaidehi, N.T.Naresh Babu, Teena Mary Treesa. An Efficient Multi-modal Biometric Person Authentication System Using Fuzzy Logic. IEEE 978-1-61284-260-8/10. 2010

[16] Nageshkumar, M. Mahesh. PK, M. N. Shanmukha Swamy. An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image. IJCSI International Jornal of Computer Sience Issues. 1694-0784, 1694-0814, 2009.

[17] Dr. Shubhamgi D C, Manohar Bali. Multi-Biometric Approaches to Face and Fingerprint Biometrics. International Journal of Engineering Research & Technology. 2278-0181. 2012.

[18] Babler, W. J. 1991. Embryologic development of epidermal ridges and their configurations. Birth Defects Original Article Series, 27(2), 95–112.

[19] Pankanti, S., Prabhakar, S., & Jain, A. aug 2002. On the individuality of fingerprints. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 24(8), 1010 – 1025.

[20] Busch, C. January 29th 2009. IMT 4621-Biometrics Course: "Biometric Systems" - script. Number Version 1.0. NISLab.

