A Review of Multibiometric System with Recognition Technologies and Fusion Strategies

Cammy Singla
M.TECH (ECE) Student
BGIET, Sangrur

Naveen Goyal
Assistant Professor
BGIET, Sangrur

ABSTRACT
Biometrics means technology of measuring and analyzing physiological or biological characteristics of living body for identification and verification purposes. A biometric system provides automatic recognition of an individual based on some sort of unique feature or characteristic of the individual. Biometric systems is based on palmprints, fingerprints, facial features, voice, signature, hand features, handwriting, the retina and iris. User verification systems that use a single biometric indicator often have to contend with noisy sensor data, restricted degree of freedom, non-universality of the biometric modalities and unacceptable error rates. So the need of modifying multimodal biometric system occurred. A multimodal biometric system have different biometric traits and provides better recognition performance as compared to the systems based on single biometric trait. This paper presents a review of multibiometric systems including its recognition technologies, level of fusion and feature extraction for fingerprint and iris. Features like minutia points from fingerprint and texture from iris are extracted.

Keywords
Biometrics, Multimodal,fingerprint,iris,recognitiontechniques,

level of fusion and feature extraction of iris and fingerprints.

1. INTRODUCTION
A biometric system provides automatic recognition of an individual based on some sort of unique feature or characteristic of the individual. Biometrics refers to the automatic identification of an individual based on his/her physiological traits [1]. Biometric systems are based on palmprint, fingerprints, facial features, voice, signature, hand geometry, handwriting, the retina and iris. Biometrics is derived from Bio (means life) and Metrics (means system used for measurement). This means that biometrics means technology of measuring and analyzing physiological or biological characteristics of living body for identification and verification purposes. Biometric systems work by first capturing a sample of the feature for example taking a digital color image for face recognition or recording a digital sound signal for voice recognition or taking fingerprint samples of fingers. Then some sort of mathematical functions are applied on the samples. The biometric template will provide an efficient and highly discriminating representation of the feature. In order to determine identity these features can be compared with other templates. Mostly biometric systems use two modes of operation. First is enrolment mode which is used for adding templates to a database and second is identification mode in which a template is created for an individual. Physiological biometrics and behavioral biometrics are two types of biometrics as shown in Fig. 1. Fingerprint recognition, facial recognition, hand geometry, iris recognition and DNA are examples of physiological biometrics where as speaker recognition, signature, keystroke and walking styles are examples of behavioral biometrics.

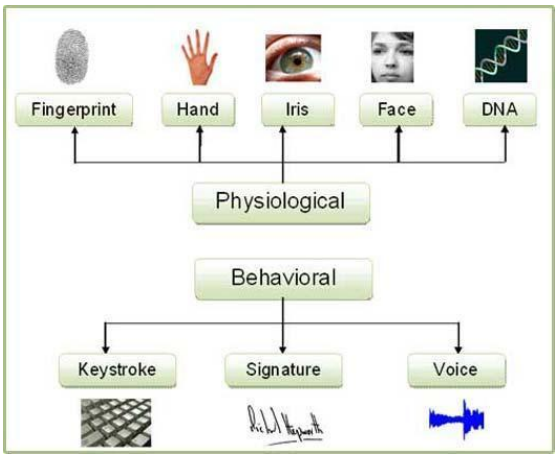


Fig. 1: Illustrations of some biometric characteristic

In uni-modal biometric systems we face a variety of problems such as noised data, intra-class variations, restricted degrees of freedom, un-universality, spoof attacks, and nonacceptable error rates [2]. The limitations imposed by uni-modal biometric systems can be overcome by using multiple sources of information for establishing identity. Such systems are called as multimodal biometric systems. These multibiometic systems are more reliable due to the presence of multiple biometric traits

2. INDIVIDUAL DISTINGUISHMENT
2.1 Fingerprint distinguishment
Unique mark distinguishment is a standout amongst the most famous and remarkable biometrics. Due to their uniqueness, fingerprints have been utilized for distinguishment for more than a century. Fingerprints are different to every individual as shown in Fig. 2 in light of an exceptional papillary gimmicks which are diverse even in twins. Unique finger impression examples stay unaltered all through the whole grown-up life and that is the reason effortlessly utilized for recognizable proof. Regardless if a finger is harmed, different fingers that are already selected into the framework can likewise be utilized for ID.

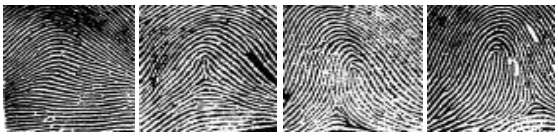


Fig 2: Cases of some biometric characteristics

Finger impression handling could be possible in two ways. Firstly utilizing equipment and furthermore utilizing programming. In equipment unique mark transforming exceptional biometric scanners are utilized to catch fingerprints. There are three sorts of unique mark scanners

which are Capacitive scanner, Clear scanner,Optical scanner. Fingerprints are distinct to each person because of a unique papillary features. The systematic study on the ridge, furrow, and pore structure (Fig.3) in fingerprints has been published in [3]. A system on fingerprint classification is discussed in [4].

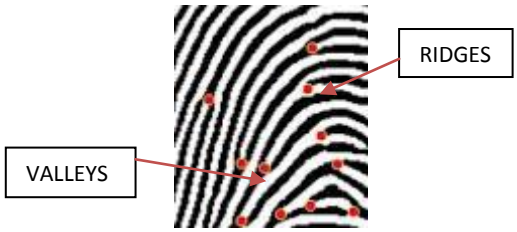


Fig 3: Rridges and valleys of fingerprints

2.2 Iris Distinguishment

Because of numerous hues, iris is known as "Goddess of the Rainbow", which is a Greek word. The slight divide between the dull understudy and white sclera is iris. The iris is the annular ring between the sclera and pupil boundary and contains the flowery pattern unique to each individual as shown in Fig. 4. In human eye iris is the hued part which is set behind the cornea.In programming transforming there are two coordinating systems. Particulars coordinating is broadly utilized distinguishment system. Details coordinating is in view of the particulars focuses, uniquely course and area of every point. In Example coordinating two pictures are just contrasted with perceive how comparative or disparate they are to one another.

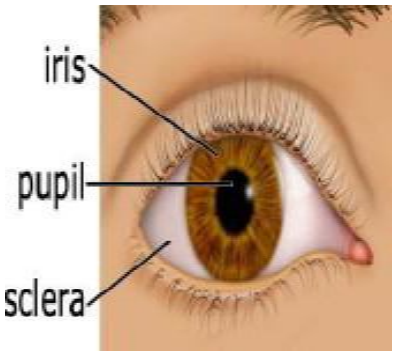


Fig 4: Human Eye

Picture handling systems can be utilized to concentrate the one of a kind iris design from a digitized picture of the eye and encode it into a biometric layout, which can be put away in a database. This biometric format contains a target numerical representation of the interesting data put away in the iris and permits correlations to be made between formats. This format is then contrasted and alternate layouts put away in a database until either a coordinating layout is discovered and the subject is recognized or no match is discovered and the subject stays unidentified.

3. LEVEL OF COMBINATION

The vital issue to planning multibiometric framework is to focus the wellsprings of data and mix systems. Contingent upon the kind of data to be melded, the combination plan can be characterized into distinctive levels. As indicated by Sanderson and Paliwal [5], the level of combination can be characterized into two categories, combination before coordinating (preclassification) and combination in the wake of coordinating (post characterization) as demonstrated in Figure 5.

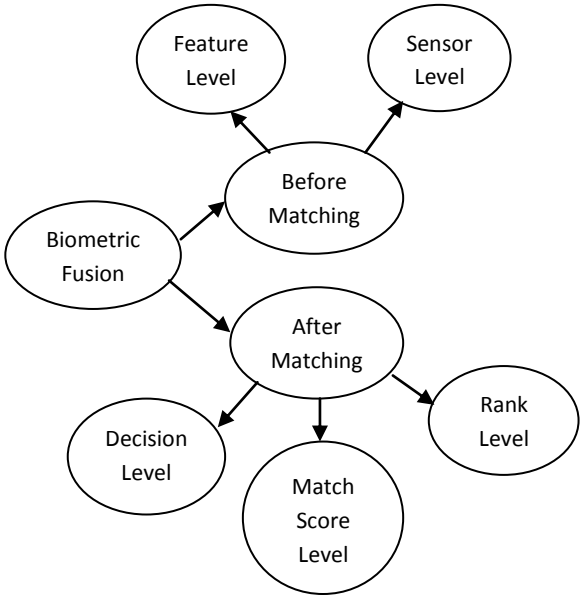


Fig 5: Level of fusion

3.1 Fusion before Matching

3.1.1 Sensor level combination

In this level, the crude information from the sensor are joined together as indicated in Fig. 6. In any case, the wellspring of data is relied upon to be debased by commotion, for example, non-uniform brightening, foundation mess and other [6]. Sensor level combination can be performed in two conditions i.e. information of the same biometric quality is gotten utilizing different sensors; or information from various depiction of the same biometric qualities utilizing a single sensor [7, 8].

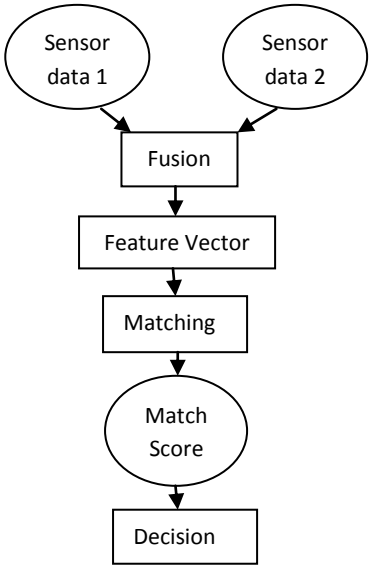


Fig 6: Sensor level combination methodology stream

3.1.2 Feature level combination

In gimmick level combination, distinctive peculiarity vectors removed from different biometric sources are joined together into a solitary gimmick vector as portrayed in Fig. 7. This methodology experiences two stages which are gimmick standardization and peculiarity determination. The gimmick standardization is utilized to adjust the area and size of peculiarity qualities by means of a change capacity and this alteration could be possible byusing fitting standardization plans [9]. For example, the min-max method and average plotting have been utilized for hand and face [10] and the mean score from the discourse flag and lipreading pictures scores have been utilized in the peculiarity level combination.

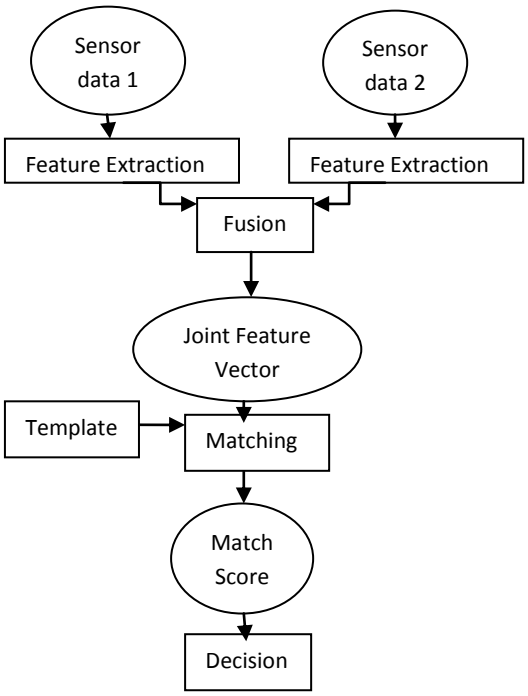


Figure 7: Feature level fusion process flow

3.2 Fusion after Matching

3.2.1 Score level combination

In score level combination, the match yields from various biometrics are joined together to enhance the coordinating execution to confirm or distinguish singular as indicated in Fig. 8 [11]. The combination of this level is the most prominent approach in the biometric writing because of its basic methodology of score accumulation and it is additionally pragmatic to be connected in multibiometric framework. In addition, the coordinating scores contain sufficient data to make genuine and fraud case recognizable [12]. However, there are some factors that can affect the combination process hence degrades the biometric performance. For example, the matching scores generated by the individual matchers may not be homogenous. Keeping in mind the end goal to finish this restriction, three combined plans have been introduced i.e. thickness based plans; change based plan; and classifier-based plan [13].

3.2.2 Decision level combination

Combination at the choice level is executed after a match choice has been made by the individual biometric source as shown in Fig. 9. In this way, there are different strategies part voting, weightedmajority voting, Bayesian choice combination, Dempster-Shafer hypothesis of proof and conduct information space [14]. On alternate hands, Ramli et al., [15] executed the proposed choice combination by utilizing the spectrographic and cepstrumgraphic as peculiarities extraction and UMACE channels as classifiers in the framework to diminish the slip because of the variety of data have been joined to connect the different choice into a definite conclusion, for example, "AND" and "OR" rules [16].

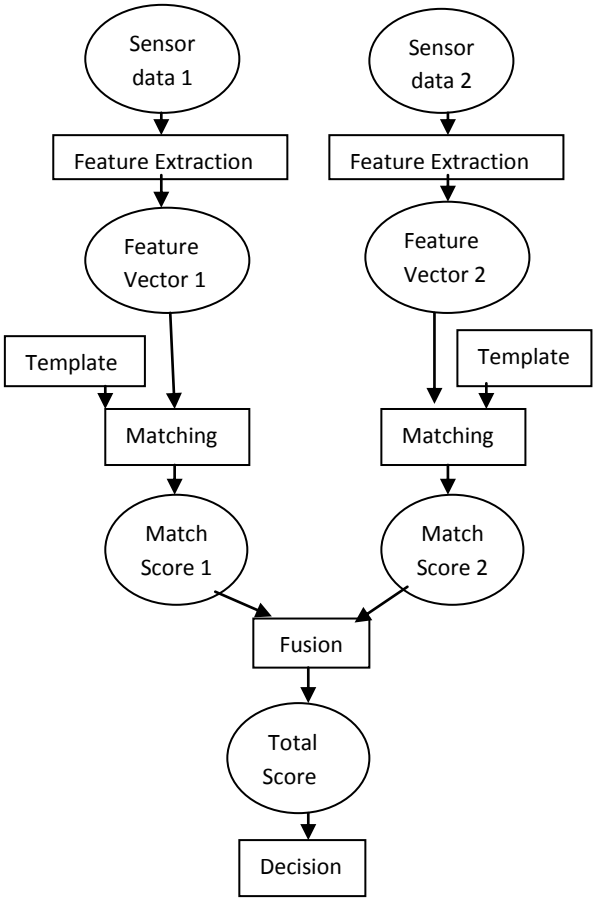


Figure 8: Score level fusion process flow

Fusion at the decision level is a rather loosely coupled system architecture, with each subsystem performing like a single biometric system. This architecture has therefore become increasingly popular with biometric vendors, often advertised under the term “layered biometrics”. Many different strategies are available to combine the distinct decisions into a final authentication decision. They range from majority votes to sophisticated statistical methods.

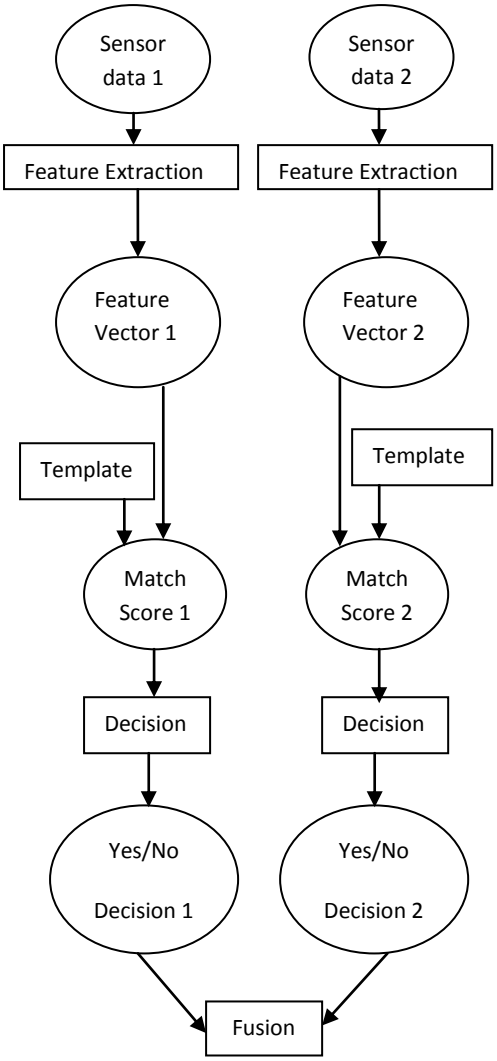


Figure 9: Decision level fusion process flow.

4. PROPOSED SCHEME

4.1 Minutiae Focuses Extraction From Fingerprints

Finger impression distinguishment is carried out by a few gimmicks, for example, minutia focuses (Bifurcation & edges). The general procedure can be separated into taking after operations:

1. Load the picture

2. Binarization

3. Diminishing

4. Minutia Extraction

5. Yield picture

Minutia Extraction as in Fig.12 is carried out by utilizing cover operation.

a) Bufrication

0	1	0
0	1	0
0	0	0

b) Ridges

0	1	0
0	1	0
1	0	1

4.1.1 Implementation of unique finger impression Recognization framework

Fig 10: Original Image

Fig 11:Thinned Image

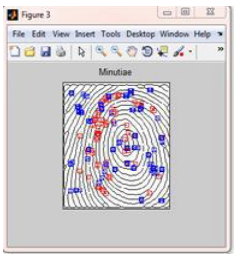


Fig 12: Fingerprint feature extraction with minutia points

4.2 Feature extraction of iris

Iris distinguishment is a compelling means for client validation. iris has a few critical characteristics like 1) Iris has exceedingly recognizing surface 2) Right eye contrasts from left eye 3) Twins have distinctive iris characteristics. The different types of steps included in peculiarity extraction of iris are as per the following:

1. Load the picture

2. Division

3. Standardization

4. Vigilant edge Detection

5. Daugman's Rubber Sheet Model

Iris characteristic extraction is gotten through of a Gabor channel. The general technique is load the eye picture into theframework extraction of gimmick in the composition form

which utilizes the Gabor channel that peculiarity is spoken to in the iris code.

Hough change used to focus geometric elements, for example, line, circles. Roundabout Hough change is utilized to recognize the span and focus directions of student and iris. The Equation for identifying the circles as takes after: k, l are the x and y coordinates, g is the range of circle defined.

$$k2+l2=g2 \quad \text{(Eq.1)}$$

For distinguishing the edges of eye watchful edge identification is utilized. It just perceives the edges from the eye picture. Presently we have confined the iris locale. For consistent measurement we are utilizing the daugman's elastic sheet model.

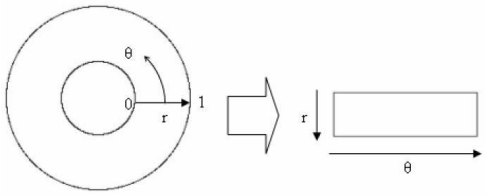


Fig 13: Daugman's elastic sheet

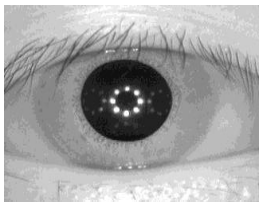
Daugman's remap the every purpose of iris locale to a polar coordinates(r,) where r is in the scope of [0, 1] and $\boldsymbol{\theta}$ is of reach [0,2pi]. The remapping of directions are carried out from circle's x and y coordinates it changes over the co-ordinates into the polar directions .The comparison is as per the following

$$R= ag \pm ag2 - a - r2$$

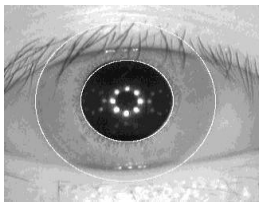
where a =$\boldsymbol{\sigma}$x2+ $\boldsymbol{\sigma}$y2

$$g= \cos (pi - \tanh - 1\sigma x2/\sigma y2) \quad \text{(Eq.2)}$$

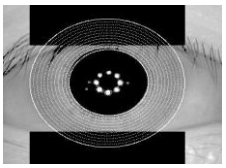
The $\boldsymbol{\sigma}$x, $\boldsymbol{\sigma}$y determines the distance of center of the iris and center of pupil. We get the result in the format of rectangular portion as shown in Fig 14 (e).



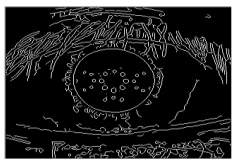
a) Original Image



b) Segmented Image



c) Normalize Image



d)Edge Detection

e)Extracted Feature of Iris

Fig 14:Different images during extraction of eye

Multimodal biometrics was gone for security-cognizant clients. Multimodal biometric framework has some great favorable circumstances, for example, 1) Improved exactness 2) Verification Or Identification on the off chance that sufficient information is not extricated from given biometric format 3) Ability to shield the classified information from Kparody assault. A few stages included in proposing the multimodal based methodology for cryptographic key era are :

1) Feature extraction from unique finger impression.

2) Feature extraction from iris.

3) Fusion of unique finger impression and iris characteristics.

4.3. Fusion of fingerprint and iris features

4.2 Fusion of fingerprint and iris features

The following step is to wire the two arrangements of peculiarities to get a multimodal biometric layout for verification. The Fused Image as shown in Fig. 15 is indicated be low: Fused Features of Two Templates (Fingerprint & Iris).These frameworks have the capacity to meet the execution prerequisites of different applications. They address the issue of non-comprehensiveness, since numerous characteristics guarantee sufficient populace scope. Mocking is unrealistic in multimodal biometric framework in light of the fact that it would be troublesome for an impostor to satire numerous biometric qualities of a real client all the while.

Fig 15: Fused Features of Two Templates (Fingerprint & Iris)

5. DISCUSSION AND CONCLUSION

Multibiometric systems are expected to alleviate many limitations of biometric systems by combining the evidence obtained from different sources using an effective fusion scheme. In this paper, the sources of biometric information were presented. The description regarding the level of fusions was also presented in this paper. From the study, it reveals that, performance of multibiometric systems can be further improved if an appropriate fusion strategy is used especially for the system which executed in uncontrolled environment Hence, a different weighting in fusion is applied to maximize the performance of multibiometric system. In our project, we have been using two modalities such as Fingerprint fusion of two modalities using principal component analysis method. Here, we got the fused biometric that fused biometric template

used for encryption using selective encryption method. Basically now a day's selective encryption method is used for encryption because it gives helpful results for multimedia data and it is will use for further applications such as compression of encrypted images on web. So, multimodal biometrics gives accuracy in providing results as compared to unimodal system. By experimental results it shows that accuracy in system of multimodal system is efficient than unimodal system.More than two modalities must combined in future work to get more powerful multibiometric system with less number of errors, better authentication will be achieved due o less errors by using appropriate fusion technology.

6. REFERENCES

[1] Jain, A.K., Ross, A., Prabhakar, S.: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics 14 (2004) 4-20

[2] Jain, A.K., Ross, A.: Multibiometric Systems. Communications of the ACM, Special Issue on Multimodal Interfaces 47 (2004) 34-40

[3] H. C. Lee, & R. E. Gaensslen, Eds., *Advances in Fingerprint Technology* (New York, Elsevier, 1991).

[4] Federal Bureau of Investigation, *The Science of Fingerprints (Classification and Uses)* (Washington, D.C., US Govt. Printing Office, 1984).

[5] C. Sanderson, and K.K. Paliwal, "Noise compensation in a person verification system using face and multiple speech features", Pattern recognition, Vol. 2, 2003, pp. 293-302.

[6] S.S. Iyengar, L. Prasad, and H. Min, Advances in Distributed Sensor Technology, Prentice Hall, 1995.

[7] R. Singh, M. Vatsa, A. Ross, and A. Noore, "Performance Enhancement of 2D Face Recognition via Mosaicing", in Proceedings of the 4th IEEE Workshop on Automatic Identification Advanced Technologies (AuotID), 2005, pp. 63–68.

[8] A. Ross, and R. Govindarajan, "Feature Level Fusion Using Hand And Face Biometrics", in Proceedings of SPIE Conference on Biometric Technology for Human Identification, Vol. 5779, 2005, pp. 196–204.

[9] A. K. Jain, K. Nandakumar, U. Uludag, and X. Lu, "Multimodal Biometrics", from Augmenting Face With Other Cues, in W. Zhao, and R. Chellappa, (eds) Face Processing: Advanced Modelling and Methods, Elsevier, New York, 2006. pp. 675-705.

[10] A. Jaina, K. Nandakumara, A. Ross, and A. Jain, "Score Normalization in Multimodal Biometric Systems", Journal of Pattern Recognition, Vol. 38, 2005, pp. 2270.

[11] A.K. Jain, and A. Ross, "Multibiometric Systems. Communications of The ACM", Special Issue on Multimodal Interfaces, Vol. 47, No. 1, 2004, pp. 34-40.

[12] M.X. He, S.J. Horng, P.Z. Fan, R.S. Run, R.J. Chen, J.L. Lai, M.K. Khan and K.O. Sentosa, "Performance Evaluation of Score Level Fusion in Multimodal Biometric Systems", Journal of Pattern Recognition, Vol. 43, No. 5, 2010, pp. 1789-1800.

[13] A. Ross, and A.K. Jain, "Fusion Techniques in Multibiometric Systems", from Face Biometrics for Personal Identification. In. R.I. Hammound, B.R. Abidi and M.A. Abidi (eds.), Publisher Springer Berlin Heidelberg, 2007, pp. 185-212.

[14] PhukeV.A, H.N.Bharathi, "Information Retrieval using Dempster-Shafer Theory" International Journal of Computer Applications (0975 – 8887) Volume 102– No.13, September 2014.

[15] R. Brunelli, and D. Falavigna, "Person Identification Using Multiple Cues", IEEE Transactions on Pattern Analysis and Machine.

[16] Intelligence, Vol. 17, No.10, 1995, pp. 955–966. C.C. Lip, and D.A. Ramli, **"**Comparative Study on Feature, Score and decision Level Fusion Schemes for Robust Multibiometric Systems", Advances in Intelligent and Soft Computing, Vol. 133, 2012, pp. 941-948.