Scientific Journal of Impact Factor(SJIF): 3.134
e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 7, July -2015

# A Proposed Multi-Model Biometrics Fusion Architecture for Authentication

Anil Kumar [1], Balraj[2], Pankaj Kumar verma[3]

[1]CSE, HCTM
[2]Research Scholars, CSE,NIILM
[3]CSE, ASRA College of Engg., Sangrur

**Abstract --** *Biometric is the good way to recognize and authenticate a person for his/her identification. Almost every field is using this biometric technique, whether it is government or private sector. In present days it is good method for enrollment and authenticates a person. Biometrics of a person can be based on physical features or behavior features of a person. It's totally depends on the choice of the person. For common applications the fingerprints method is a good choice. But for more secure applications, Uni-biometric system is not sufficient. For more security multi-biometric may be implemented. A framework needs to be developed for integrating multiple cues for making biometric system totally foolproof. In the proposed work, i will work on Multi-model Fusion Architecture for Face and fingerprint authentication and using NN. Later the Proposed technique will be compared with SVM to enhance the performance on the basis of CCR, MSE and PSNR.*

***Keywords***- *NN, SVM, Fingerprint, Face, CCR.*

## I. INTRODUCTION

In biometrics a person may be identified by his/her fingerprints and can authenticate for some work. Authentication of a person by the fingerprints required extraction of the fingerprint for matching purpose. There are some algorithms which help to extract the fingerprint features such as minutia based, pattern based etc. It is base on the choice of the user any algorithm can be used. A person can also be identified by his/her face also in this case facial features are extracted and matched against the database templates. But all these are Uni-Biometric techniques. Recognition of a person can also be done using Multi-biometric technique. In Multi-biometric system two or more biometric features can be combined to create a multi-model biometric.

## II. UNI-BIOMETRICS

Biometrics system is recognition and the identification of an individual on the basis of physiological or behavioral characteristics of a person such as iris, palmprints, face, voice and fingerprints as shown in figure 1. Biometrics word arrived from the Greek words bios (Life) and metricos (Measure). It is basically a pattern-recognition system that is used to identify a user and relies on something that is a part of a person's biological makeup of behavior, such as a face, signature or a fingerprint.

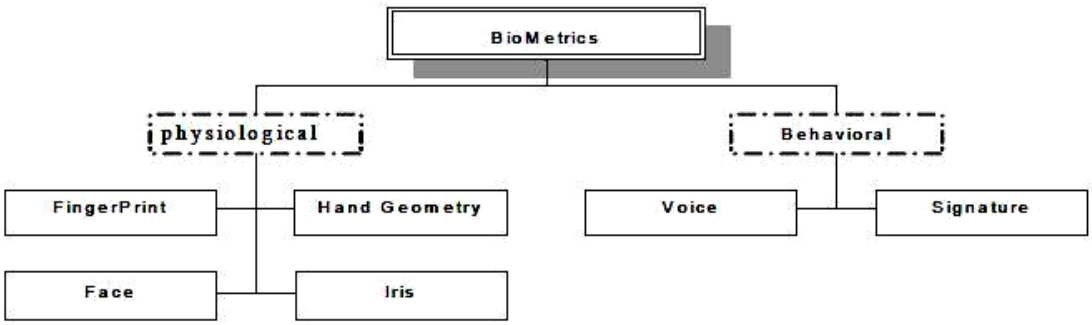


**Figure1:** Common Biometrics features [1].

## III. MULTI-BIOMETRICS

Multimodal biometric systems are those biometric systems which are capable of utilizing, more than one physiological or behavioral features of a person for enrollment, verification, or identification. Multimodal biometrics is the combination of two or more biometric features of human being for verification and Identification. The most convincing reason to combine different biometric features is to improve the recognition rate. A multi-biometric system offers extensive improvement in the accuracy of a biometric system but it is depends on the features being combined and the fusion method is adopted [2]. Multi-biometric systems can alleviate many of the limitations of uni-modal biometric systems because the different biometric sources usually compensate for the inherent limitations of the other sources [3].

### 3.1 Multi-Biometric Categories

 

**3.1.1 Multi sensor.**
In this system multiple sensors can be used to collect the same biometric trait.

**3.1.2 Multi-modal.**
This is our proposed are of work here multiple biometric traits of the same person are collected e.g. palmprint, fingerprint, iris and face etc.

**3.1.3 Multi-instance.**
Multiple units of the same biometric are collected, e.g. iris scan of left or right eye fingerprints from two or more fingers.

**3.1.4 Multi-sample.**
Multiple capturing of the same biometric trait are collected during the enrolment and/or authentication phases, e.g. a number of face capturing are taken at different pos and illumination.

## IV. FINGERPRINT RECOGNITION

Fingerprint recognition is also known as "image acquisition". In this part of the process, a user places his or her finger on a scanner. Numerous images of the fingerprint are then captured. It should be noted that during this stage, the goal is to capture images of the center of the fingerprint, which contains many of the unique features. All of the captured images are then converted into black and white images.

## V. FACIAL RECOGNITION

It means identification of a person by his facial characteristics. Facial recognition is one of the most common biometric methods of identification. Here facial features of a person are detected and extracted from an input image. In addition, the method of acquiring face images is non-intrusive. Two primary approaches to the identification based on face recognition are the following: (i) Transform approach: the universe of face image domain is represented with a set of orthonormal basis vectors. Nowadays, (ii) eigenfaces is the most popular basis vector.

## VI. FUSION

Generally the meaning of fusion is to extraction of features or some information in several domains. In Biometric fusion can be defined generally as the use of multiple types of biometric data of processing to improve the performance of biometric systems or we can say for the improvement of biometric system multiple biometric input/data/methods are used. Its key purposes are to improve system accuracy, efficiency, applicability, and robustness. Multi-sensor [4] image fusion means combining information from two or more images into a single image called fused image. The goal of image fusion (IF) is to combine balancing multi-sensor, multi-temporal and/or multi-view information into one new fused image containing information the quality of which cannot be achieved otherwise. This technique is applied on several images of the same scene, than it will provide a new image with higher quality.

## VII. LITERATURE REVIEW

**R. Snelick et al (2003)** [5] Experimental studies show that multimodal biometric systems for small-scale populations perform better performance than single-mode biometric systems. We examine if such techniques scale to larger populations, introduce a methodology to test the performance of such systems, and assess the feasibility of using commercial off-the-shelf (COTS) products to construct deployable multimodal biometric systems. A key aspect of our approach is to leverage confidence level scores from preexisting single-mode data. An example present a multimodal biometrics system analysis that explores various normalization and fusion techniques for face and fingerprint classifiers. This multimodal analysis uses a population of about 1000 subjects, a number ten-times larger than seen in any previously reported study. Experimental results combining face and fingerprint biometric classifiers reveal significant performance improvement over single-mode biometric systems.

**Austin Hicklin et al (2006)** [6] Biometric fusion is the use of multiple biometric inputs or methods of processing to improve performance. The key purposes for biometric fusion are to improve system accuracy, efficiency, applicability, and robustness. Some types of fusion have been used successfully for years in large scale fingerprint identification systems. While fusion can be very effective, it should not be regarded as a panacea, since it adds complexity to data collection and system architecture.

**Jan Flusser et al (2007)** [7] authors present a survey of traditional and up-to-date registration and fusion methods and demonstrate their performance by practical experiments from various application areas. Special attention is paid to fusion for image restoration, because this group is extremely important for producers and users of low-resolution imaging devices such as mobile phones, camcorders, web cameras, and security and surveillance cameras.

**E. Camlikaya et al (2008)** [8] as biometrics gains popularity, there is an increasing concern about privacy and misuse of biometric data held in central repositories. Furthermore, biometric verification systems face challenges arising

 

from noise and intra-class variations. To tackle both problems, a multimodal biometric verification system combining fingerprint and voice modalities is proposed. The system combines the two modalities at the template level, using multi-biometric templates. The fusion of fingerprint and voice data successfully diminishes privacy concerns by hiding the minutiae points from the fingerprint, among the artificial points generated by the features obtained from the spoken utterance of the speaker. Equal error rates are observed to be under 2% for the system where 600 utterances from 30 people have been processed and fused with a database of 400 fingerprints from 200 individuals. Accuracy is increased compared to the previous results for voice verification over the same speaker database.

**S. Anu, H Nair et al (2014)** [9] Image Fusion is a process of integrating multiple images into a single image. Biometric features are used to provide authentication and security of systems. This paper deals with a new work that implements fusion of biometric features like iris and palmprint. The iris and palmprint are transformed into the set of features independently. The extracted modalities are fused by different fusion algorithm techniques like the pyramid based algorithms and wavelet based algorithms. The quality of fused images is assessed using metrics such as Visual information fidelity, Qabf, Peak Signal Noise Ratio, Mutual Information, Mean Square Error, Normalized Absolute Error, Normal Correlation Coefficient, Cross entropy and Relative Warp. Comparative evaluation of fused images is a critical step to evaluate the relative performance of different image fusion methods. The fused template can be further used in applications like watermarking, person identification system.

## VIII. PROPOSED ARCHITECTURE DESIGN

As in fingerprint matching technique matching algorithms compare the previously stored image templates against a candidate fingerprints for authenticity. My proposed work is same but with multimodal biometric system using NN_SVM. In this proposed algorithm my concentration is on physiological fingerprint and face recognition methods. I have considered both objects as images, fused and stored those images in a database as templates. Whenever we have to check the authenticity of a person we will scan his fingerprint and photo using a scanner/digital camera. These new objects will be fused and compared with our created database using NN and SVM. The complete process of this proposed work is divided into three main modules load module, Fusion module and the Matching module as shown in figure 3 and figure 3 is showing the flow chart of the proposed architecture.

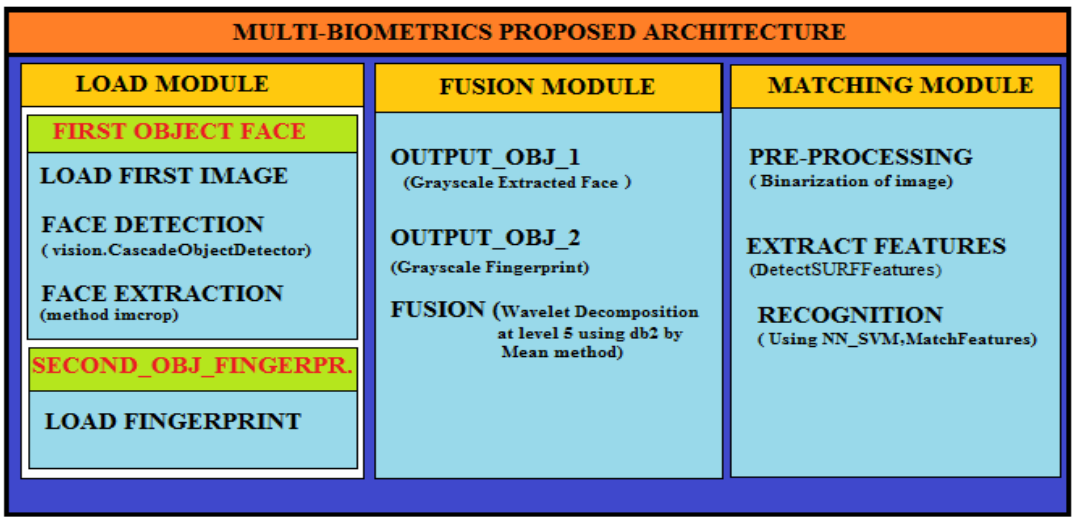


**Figure 2:** Multi-Modal Biometric Proposed Architecture.

Next figure is showing the flow chart of our proposed model

 

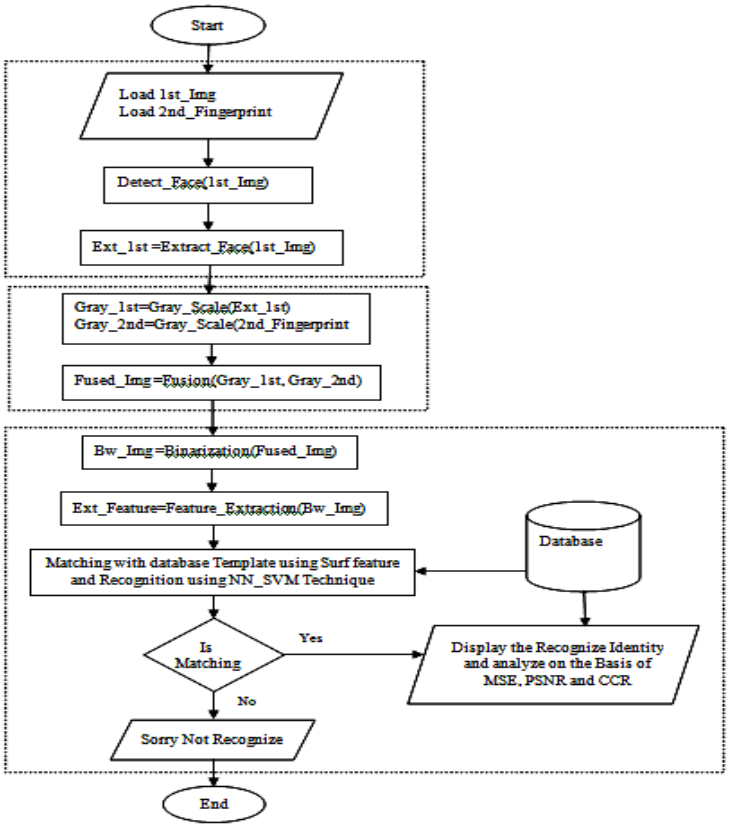


**Figure 3**: Flowchart of proposed algorithm

## IX. RESEARCH METHODOLOGY

This is the methodology used to implement this research work.

### 9.1 Neural Network (NN)

Neural networks are composed of simple elements operating in parallel. These elements are inspired by biological nervous systems. As in nature, the connections between elements largely determine the network function. You can train a neural network to perform a particular function by adjusting the values of the connections (weights) between elements. In addition to function fitting, neural networks are also good at recognizing patterns. nprtool leads you through solving a pattern-recognition classification problem using a two-layer feed-forward patternnet network with sigmoid output neurons. Finally we will analyze the results between fused images and recognized using MSE and PSNR and CCR [10].

### 9.2 Support Vector Machine (SVM)

It is a supervised learning models with associated learning algorithms that analyze data and recognize patterns, used for classification and regression analysis. Given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples into one category or the other, making it a non-probabilistic binary linear classifier.

**SVM Algorithm**

**Algorithm** Simple SVM
CandidateS-{closest pair from opposite classes}
**While** there are violating points **do**
Find a violator
candidateS=candidateSUviolator
**if** any αρ<0 due to addition of c to $ **then**
candidateSV = candidateSV\p
repeat till all such points pruned
**endif**

## X. CONCLUSION

At the last we can see that our proposed architecture is the combination of two biometrics features of a human being hence it will be more secure than the uni-biometrics model. For high accuracy and to increase the performance we are using two techniques collectively.

 

## XI. ACKNOWLEDGE

Thanks to my research supervisor and family member who always support, help and guide me during my dissertation. Special thanks to my father who always support my innovative ideas.

## REFERENCES

[1] Kumar, A., Ravikanth, C.: Personal authentication using finger knuckle surface. IEEE Trans. Information Forensics and Security 4(1), 98–109 (2009).

[2] Andrew Teoh, S. A. Samad and A. Hussain, "Nearest Neighbourhood Classifiers in a Bimodal Biometric Verification System Fusion Decision", Journal of Research and Practice in Information Technology, Vol. 36, No. 1, February 2004.

[3] L. Hong, A. K. Jain, and S. Pankanti. Can Multibiometrics Improve Performance? In Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies (AutoID), pages 59–64, New Jersey, USA, October 1999.

[4] M.I. Smith, J.P. Heather, "Fusion Technology Review of Image," Proceedings of the SPIE, Vol. 5782, pp. 29-45, 2005.

[5] R. Snelick, M. Indovina, J. Yen, and A. Mink. Multimodal Biometrics: Issues in Design and Testing. In Proceedings of Fifth International Conference on Multimodal Interfaces, pages 68–72, Vancouver, Canada, November 2003.

[6] Austin Hicklin, Brad Ulery and Craig Watson "A Brief Introduction to Biometric Fusion"in National Institute of Standards and Technology 16 June 2006.

[7] Jan Flusser, Filip ˇSroubek, and Barbara Zitov´a "Image Fusion:Principles, Methods, and Applications" A tutorial, Institute of Information Theory and Automation, 2007.

[8] E. Camlikaya, A. Kholmatov, and B. Yanikoglu. Multimodal Biometric Templates Using Fingerprint and Voice. In Proceedings of SPIE Conference on Biometric Technology for Human Identification V , Orlando, USA,March 2008.

[9] S.Anu H Nair and Dr.P.Aruna "Image fusion techniques for iris and palmprint biometric system" Journal of Theoretical and Applied Information Technology Vol. 61 No.3, ISSN: 1992-8645 31st March 2014.

[10] Matrix Laboratory 12.0 Help.

 