International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 8 177 - 179

Comparison Fusion of Iris and Fingerprint Traits for Personal Authentication using Artificial Neural Network with Previous Algorithm

Er. Gurnam Singh, Mr. Anurag Rana
Dept. of Computer Science and Engineering, Arni University Katgarh

Abstract— Biometrics is the science of determining the identity of a person based on the physiological / behavioral characteristics of the individual. A person can be identified by using biometrics based on 'what you are' rather than 'what you possess' such as ID card or 'what you remember' such as password . Biometrics are incorporated in many different applications because of the need for reliable user authentication techniques has increased in the wake of heightened concerns about security, and rapid advances in communication, networking and mobility . A variety of biometric characteristics including face, fingerprint, palm print, iris, retina, signature, gait, ear, hand vein, voice pattern, odor or DNA are being used in various applications. Each biometric has its merits and demerits. Therefore, the selection of a biometric trait depends on several issues other than matching performance.

Keywords:- *Biometrics, Multimodal, Face, Fingerprint, Iris, Signature, Fusion, Matching score*

*****

I. INTRODUCTION

The need for reliable user authentication techniques has increased in the wake of heightened concerns about security and rapid advancements in networking, communication, and mobility. A wide variety of applications require reliable verification schemes to confirm the identity of an individual requesting their service. Traditional authentication methods using passwords (knowledge-based security) and ID cards (token based security) are commonly used to restrict access to a variety of systems. However these systems are vulnerable to attacked and security can be easily breached. The emergence of biometrics technologies is replacing the traditional methods as it has addressed the problems that plague these systems.

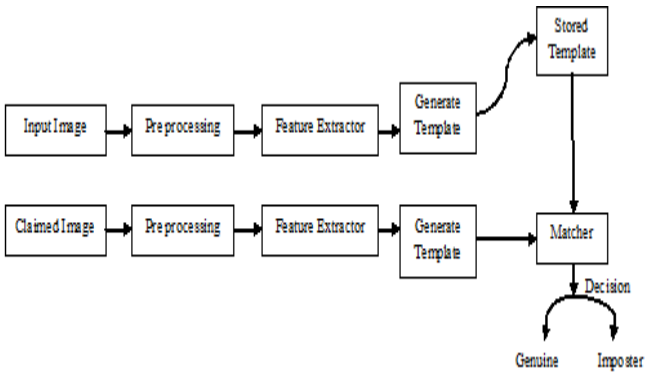

Figure 1: Basic Block Diagram of Biometric System

Biometrics refers to the authentication techniques that rely on measurable physiological and individual characteristics that can be automatically verified. Biometric-based solutions are able to provide for confidential transactions and personal data privacy . Multibiometric integrates different biometric systems for verification in making a personal identification. This system takes advantage of the capabilities of each individual biometric. These systems can expect more accuracy due to the fact that they use multiple biometric modalities where each modality presents independent evidence to make a more informed decision. Multimodal biometric systems capture two or more biometric samples and use fusion to combine their analyses to produce a better match decision by simultaneously decreasing the FAR and FRR. All unimodal biometric systems can be used with combination of others to form a multimodal biometrics. For example:

a. Speech and Signature
b. Palm veins & Signature
c. Face & Signature

II. CHALLENGES IN BIOMETRIC SYSTEMS

In recent years, biometric systems have been successfully deployed in a number of real-world applications (e.g., airports, amusement parks, banks, defenses establishments etc.) with some biometrics offering reasonably good performance. However, even the most advanced biometric systems to date are still facing numerous problems associated with a variety of factors including data, algorithm used and system design .Generally the following factors are the main drawbacks of biometric systems:

1. Noisy data
2. Non-universality
3. Lack of individuality
4. Intra-class variation
5. Susceptibility to circumvention
6. Privacy

III. PERFORMANCE METRICS OF BIOMETRIC SYSTEMS:

Expressing the performance of a biometric system requires some parameters. A decision made by a biometric system is either a "genuine individual" type of decision or an "impostor" type of decision For each type of decision, there are two possible outcomes, true or false Therefore, there are a total of four possible outcomes: a genuine individual is accepted or a genuine match occurred, a genuine individual is rejected or a false rejection occurred, an impostor is rejected or a genuine rejection occurred and an impostor is accepted or a false match

occurred . The confidence associated with different decisions may be characterized by the genuine distribution and the impostor distribution, which are used to establish two error rates:

i) False accept rate (FAR), which is defined as "the probability of an impostor being accepted as a genuine individual" . That is, in a biometric authentication system, the FAR is computed as the rate of number of people is falsely accepted (false people are accepted) over the total number of enrolled people for a predefined threshold.

ii) False reject rate (FRR), which is defined as "the probability of a genuine individual being rejected as an impostor". That is, in a biometric authentication system, the FRR is computed as the rate of number of people is falsely rejected (genuine people are rejected) over the total number of enrolled people for a predefined threshold.

IV. DESIGN & IMPLEMENTATION

This work focuses to implement the Multimodal Biometric System that provides accuracy at limited cost in terms of acquisition time. Each biometric system must perform four basic tasks i.e. acquisition, feature extraction, matching and decision making. Among these the major consideration is on feature extraction. As the number of features increases, the intrapersonal model variability issue arises, which is detrimental to system performance and chances of forgery will also increase .

1.1 Proposed Model:-

The proposed model focuses on following four objectives which are helpful in improving the efficiency of the system and are practically implemented using MATLAB 7.11.0 environment.

a) To Collect the Signature & Speech Samples in data acquisition.
b) To propose a new algorithm/method for feature level fusion.
c) To modify the algorithm for feature extraction in multimodal biometric system.
d) Compare this technique with the current state of art techniques.

A multimodal biometric system constitutes of Iris and Fingerprint acquiring device for generating digital signals and signatures. Simple system architecture is opted as shown in Fig. 2 where both streams of data using feature extraction and modelling tools are modelled independently. The feature vectors are fused using a proposed technique & obtain a new feature vector which can be stored in database. After storing all data, matcher can be used to match the new data with existing database & gives the results.

Algorithm for proposed work**:**

STEP 1: Input the Sample of fingerprints and sample of iris
STEP 2: Extract the Gabor Feature of iris and fingerprints.
STEP 3: Apply Wavelet Fusion on Extracted Feature.
STEP 4: Apply neural Network's Cascaded feed forward Back propagation Algorithm to Train Neurons for recognition
STEP 5: Evaluate the parameters of testing sample along with the parameters of trained neural network parameters.

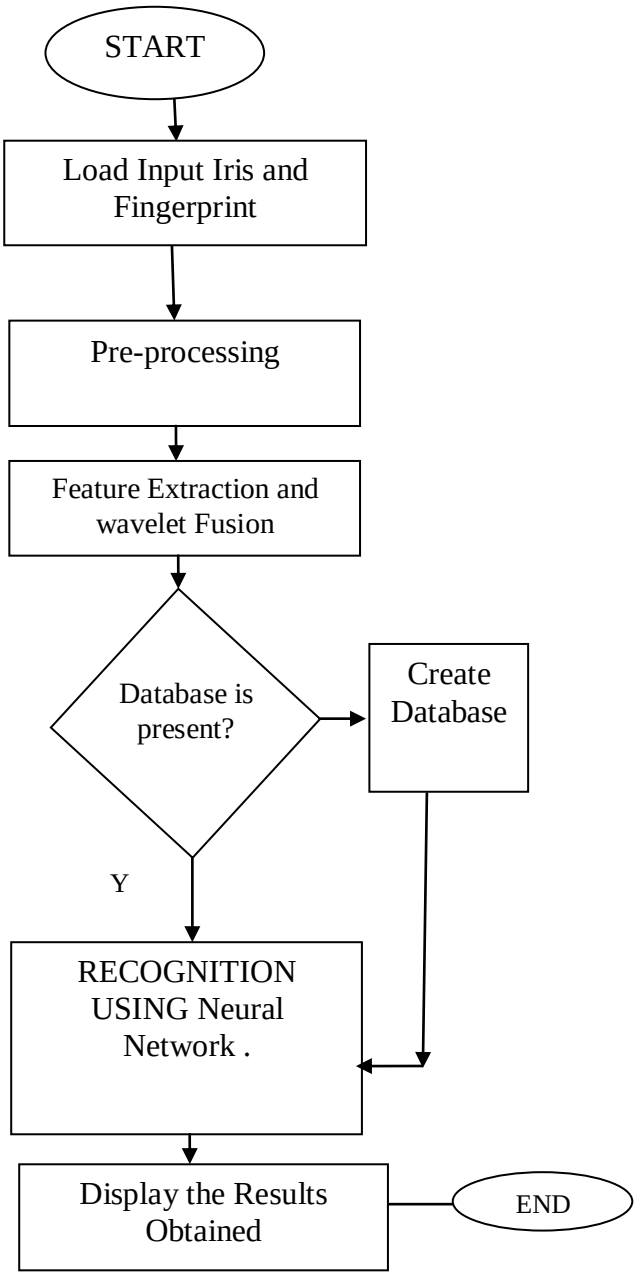

Figure 2: Flow chart for Proposed Work

V. COMPARISON WITH PRE-EXISTING ALGORITHMS

The proposed algorithm has been evaluated on virtual database of iris and fingerprints of sixteen different persons. The experiments are conduct matlab with image processing toolbox and on machine core 2 Duo CPU Processor. Table explains the comparison of various modalities combinations and their respective recognition percentage. From the above comparison we can conclude that proposed feature level wavelet fusion train by neural network is comparable with all the methods mentioned.

TABLE 1: COMPARISON TABLE

Method	Recognition Percentage	Modalities
PCA	79.79	Face and Palm print
Single scale LBP	81.46	Face and Palm print
Multiscale LBP	94.79	Face and Palm print
DICA	95.83	Face and Palm print
Modified multiscale LBP	96.67	Face and Palm print
Feature fusion	95	Face and Palm print
Multiple feature extraction	98.82	Fingerprint and Palmprint
Wavelet fusion and train by neural network	99.8	Fingerprint and iris
Integration of Iris and Fingerprint Traits for Personal Authentication	99.9	Fingerprint and iris

From the above Discussion it was observed that the experimental results demonstrated that the proposed multimodal biometric system achieves a recognition accuracy of 99.90.

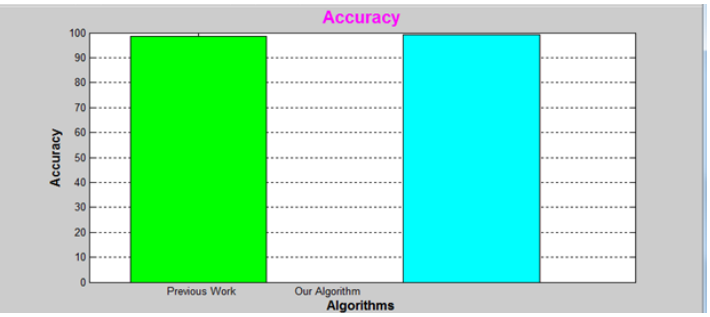

Figure 3: Comparison of Accuracy with previous algorithm

Our results show better accuracy than previous results.

2. Conclusions

The Research starts by introducing biometric and its importance in the current world. Biometric systems and challenges for these systems are also presented in this paper . Then the focus and scope of my research are defined with the Research paper contributions. A very brief methodology for the proposed multimodal biometric system is also presented in this Research Paper.Then the Focus of my research comparison with earlier algorithim.

VI. FUTURE RESEARCH DIRECTION

The outcomes of this research have been published and presented through important venues, such as International Journal of Biometrics, national Conference etc. and have benefited both academic and enterprise applications. There are some issues and open questions left for future research.

REFERENCES:

[1]. A. Ross, & A. K. Jain, Information Fusion in Biometrics, *Pattern Recognition Letters, 24*(13), 2003, 2115-2125.
[2]. W. Yunhong, T. Tan, & A. K. Jain, Combining Face and Iris Biometrics for Identity Verification, *Proceedings of Fourth International Conference on AVBPA*, Guildford, UK, 2003, 805-813.
[3]. S. C. Dass, K. Nandakumar, & A. K. Jain, A Principled Approach to Score Level Fusion in Multimodal Biometric Systems, *Proc. of Audio- and Video-based Biometric Person Authentication (AVBPA)*, Rye Brook, NY, 2005.
[4]. G. Feng, K. Dong, D. Hu, & D. Zhang, When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy, *International Conference on Bioinformatics and its Applications*, Hong Kong, China, 2004, 701-707.
[5]. L. Flom, & A. Safir, Iris Recognition System, U.S. Patent No. 4641394, 1987.
[6]. J. G. Daugman, High confidence visual recognition of persons by a test of statistical independence, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *15*(11), 1993, 1148–1161.
[7]. W. W. Boles, & B. Boashah, A Human Identification Technique Using Images of the Iris and Wavelet Transform, *IEEE Transaction on Signal Processing*, *46*(4), 1998, 1185-1188.
[8]. R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey, & S. McBride, A Machine vision System for Iris Recognition, *Machine Vision and Applications*, *9*(1), 1996, 1-8.
[9]. A. E. Hassanien, & J M. Ali, An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory, *Advanced Modeling and Optimization Journal*, *5*(2), 2003, 93-104.
[10]. H. C. Lee, & R. E. Gaensslen, Eds., *Advances in Fingerprint Technology* (New York, Elsevier, 1991).
[11]. Federal Bureau of Investigation, *The Science of Fingerprints (Classification and Uses)* (Washington, D.C., US Govt. Printing Office, 1984).
[12]. L. Hong, Y. Wan, & A.K. Jain, Fingerprint Image Enhancement: Algorithm and Performance Evaluation, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *20*(8), 1998, 777-789.
[13]. Raymond Thai, Fingerprint Image Enhancement and Minutiae Extraction, *Technical Report*, The University of Western Australia, 2003.
[14]. A. K. Jain, K. Nandakumar, & A. Ross, Score Normalization in multimodal biometric systems. *The Journal of Pattern Recognition Society*, *38*(12), 2005, 2270-2285.