IJESMR

International Journal OF Engineering Sciences & Management Research

MULTIMODAL BIOMETRIC SYSTEM USING THREE BIOMETRIC TRAITS

Ms.Priya N. Ghotkar*, Mr. Vikas G. Bhowate
* Department of Information Technology, St. Vincent Pallotti College of Engineering & Technology, Nagpur, India

KEYWORDS: Biometrics, Person authentication, Unimodal, Multimodal, Fusion

ABSTRACT
In our day to day life, the automatic verification of person is a very important task. The traditional method of establishing a person's identity include knowledge based like password or token based like ID cards, but representation of these identity can easily be lost, stolen or shared. So for authentication of a person some biometric characters of that person is used. For that purpose one or more biometric characters can be used. But using one character may sometime prove less secure so more than one characters are used. Sometimes it is possible that some people with some disability may not register or authenticate himself, in that case multimodl biometrics is essential. Some research and security related issues are mentioned here.

INTRODUCTION
In today's world where the technology is emerging rapidly, there are several *person authentication* related issues that need to be handled in daily life. Biometric is the Greek word in which *bios* (life) and *metron* (measure), and hence biological measurement is termed as *biometric*. It refers to the person's physiological or biological characteristics in which physiological characters are face, speech, fingerprint, iris, etc or behavioural characters are signature, gait or speech too. Physiological biometrics are related to the shape of the body and are generally more stable. Behavioural biometrics are related to the behaviour of the person and are comparably less stable. Hence, a proper selection of biometrics is more important than building a person authentication system using the same. The block diagram of biometric based person recognition system is given in Figure 1.

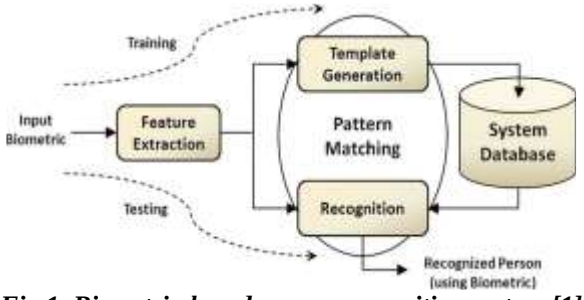

Fig 1. Biometric-based person recognition system.[1]

For training any person authentication system, the biometric data are processed for feature extraction. The most important aspect of any biometric-based authentication system is the selection of an proper feature set which should be reasonably invariant with different degradations. Modeling is done to make the template in such a way that it should hold all the variations captured by that particular biometric for every person. In the testing phase, same features are computed from the unknown test biometric template and then compared with the models of each person. This is accomplished in the pattern matching stage. Finally, after pattern matching, we get the acceptance or rejection of the person as the output result.[2]

MULTIMODAL BIOMETRIC SYSTEMS
Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity [3]. Such systems, known as *multimodal biometric systems*, are expected to be more reliable due to the presence of multiple, (fairly) independent pieces of evidence [4]. These systems are able to

IJESMR
International Journal OF Engineering Sciences & Management Research

meet the performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a 'live' user is indeed present at the point of data acquisition.

Fig 2. Multimodal Biometric System[3]

The reason to combine different modalities is to improve recognition rate. The aim of multimodal biometrics is to reduce one or more of the following:

- False accept rate (FAR)
- False reject rate (FRR)
- Failure to enroll rate (FTE)
- Susceptibility to artefacts or mimics

Multi modal biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. For example a system with fingerprint and face recognition would be considered "multimodal" even if the "OR" rule was being applied, allowing users to be verified using either of the modalities [5].

PROPOSED SYSTEM

Multimodal biometrics refers to the use of combinations of two or more biometric modalities in an identification system. Identification based on multiple biometrics represents an emerging trend. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent. There are other reasons to combine two or more biometrics. Another reason is simply customer preference. The fusion of Iris, Fingerprint and Signature at feature level is using a unique technique. The features of Iris, Fingerprint and Signature are extracted after the processing of normalized image & histogram equalization accordingly. A key is applied to perform encryption and fusion of these three feature vectors are combine. The query image feature vectors are fused and then compared with the fused feature vectors stored in the database. The final decision that if the user is genuine or imposter is taken with the help of Hamming distance matcher method.

Implementation of the biometric technology is the very challenging task for our system. Apart, of using biometric template we have implemented fusion of three biometric templates and that template also used with the algorithm for encryption technique. The interconnection of this technique is very useful for reproducing the accuracy and security of the biometric template. Now a day we have deployment of biometric system in every industries, companies and colleges. As we are all having knowledge regarding the biometric system that biometric system is used for recognition of person. But when we have analyzed different biometric system they have to face problems in using biometric system if user template fails to detect the template at the time of matching[6].

IJESMR
International Journal OF Engineering Sciences & Management Research

To improve the performance, accuracy of the system and reduce the complexity of database we have proposed multibiometric system with cryptography key. The main objective of this work is to give security to the biometric template. The proposed approach is to use three modalities i. e. Fingerprint biometric trait, Iris Biometric trait and Signature Biometric trait. The biometric system is basically is used for pattern recognition so here also we are recognizing the patterns of biometric system as an features format and that features are fused with principal component analysis. Implementation of fused image is used for encryption. The encrypted image is stored in database as a record.

Fig 3. Implementation of Template Security with Cryptography Key.

The above figure is the implementation of our multimodal biometric system. Working scheme of our system is, first step consists of performing the image acquisition of various biometric templates. The next step involves the feature extraction from the biometric traits. The extracted features are stored in the database that template have to be compared with the template stored in the database. Result is obtained as a matching score of that template.

3.1 Advantages of Proposed System

1. Compared to uni-biometric systems that rely on a single biometric trait, multi-biometric systems can provide higher recognition accuracy and larger population coverage.
2. Someone who is with certain disability will also be able to register himself using any one biometric trait.
3. Consequently, multi-biometric systems are being widely adopted in many large-scale identification systems.

3.2 Data flow of system

In above given data flow diagram, we take three biometric inputs i.e.Iris, Fingerprint and signature after that we apply different pre processing steps to makes it more efficient. Then next step in data flow diagram is feature extraction .The proposed framework does not put any particular restriction on the type of modality or the feature extractor utilized. It should however be kept in mind during the design of the feature extractors that their output must conform with the input requirements of the selected matcher. In this project, the wavelet iris for iris feature extraction and wavelet fingerprint for FP feature extraction the extracted feature is of size 1 X 60.

IJESMR
International Journal OF Engineering Sciences & Management Research

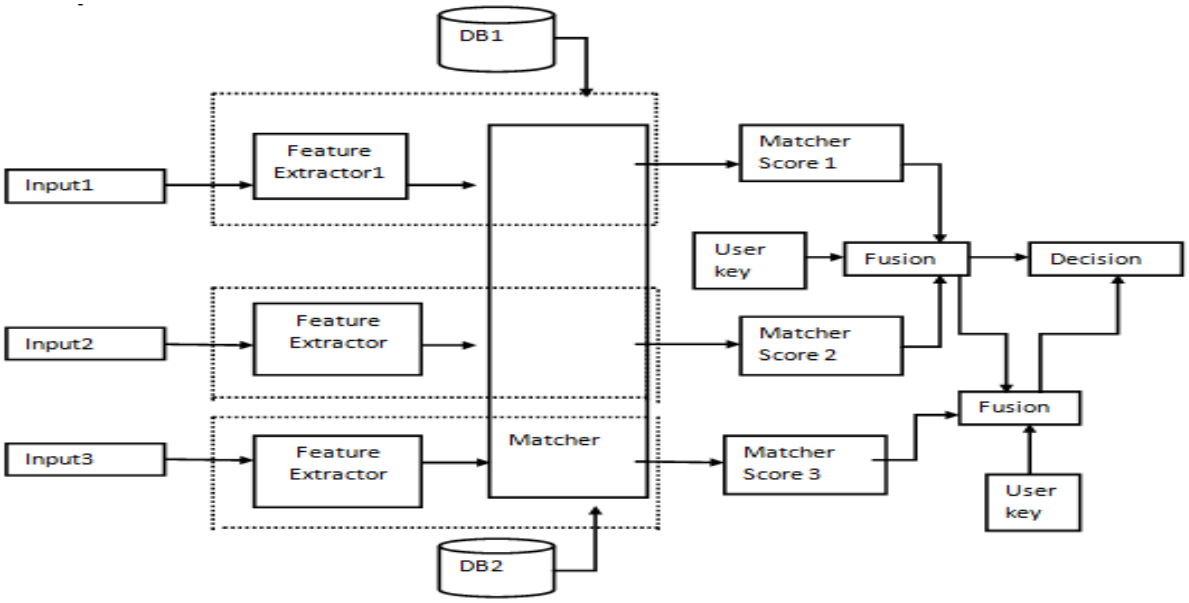

Fig 4: Data Flow Diagram of Proposed System

RESULT AND ANALYSIS

While executing the system following are the snapshots. After loading the three biometric traits in the system, the person get registered himself. In this proposed method 20x20 tolerance square is used during user registration process. 10 samples are taken to calculate the total time required for database creation and evaluation. Fig 5. shows the snapshot while registering and fig 6. shows the snapshot while authentication.fig 7. shows the total time required for database creation and database evaluation.

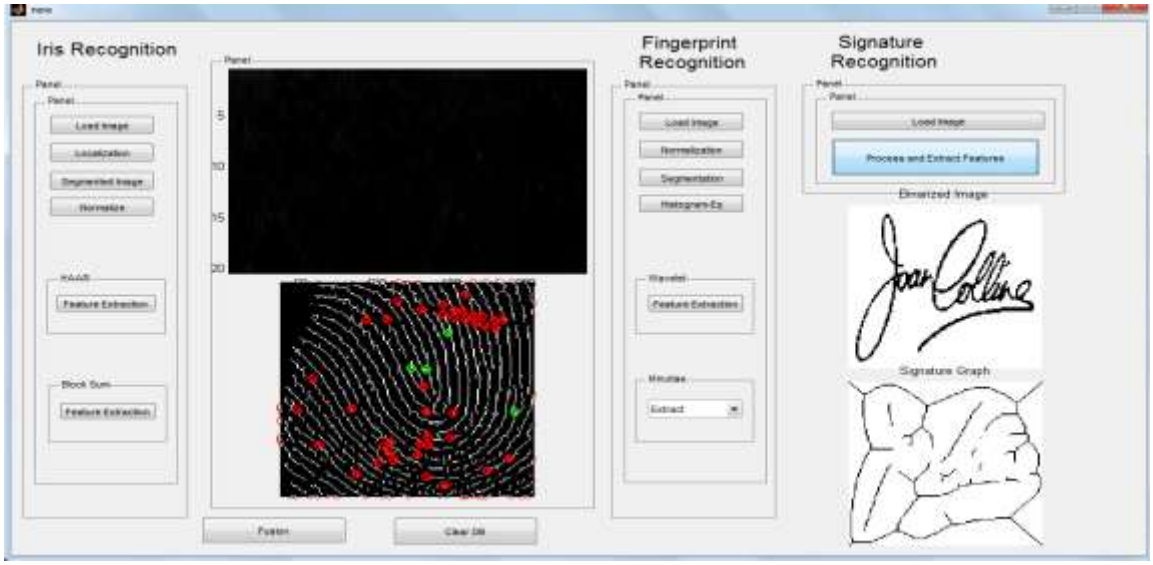

Fig 5. Snapshot for database creation

IJESMR
International Journal OF Engineering Sciences & Management Research

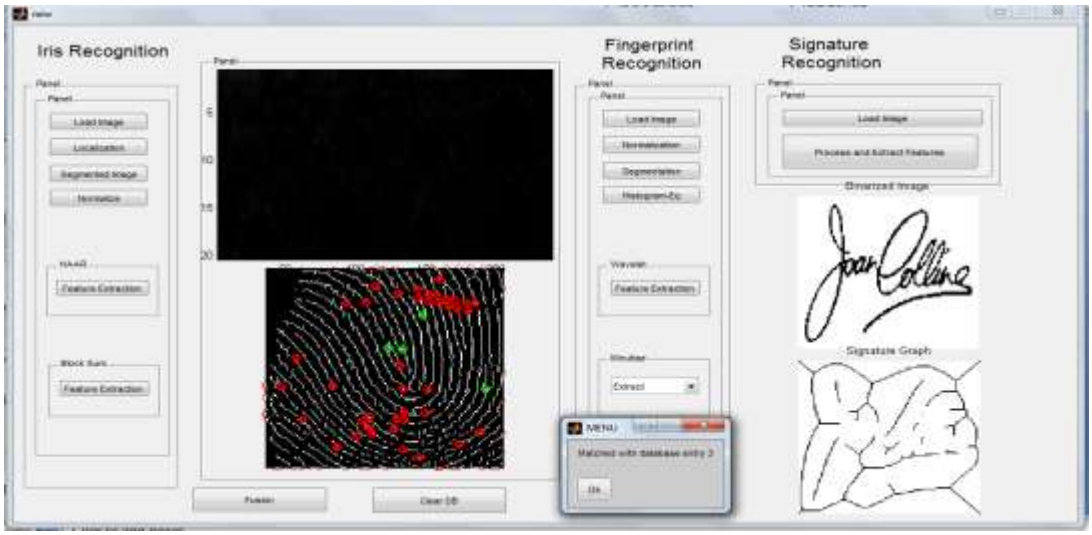

Fig 6. Snapshot for database matching

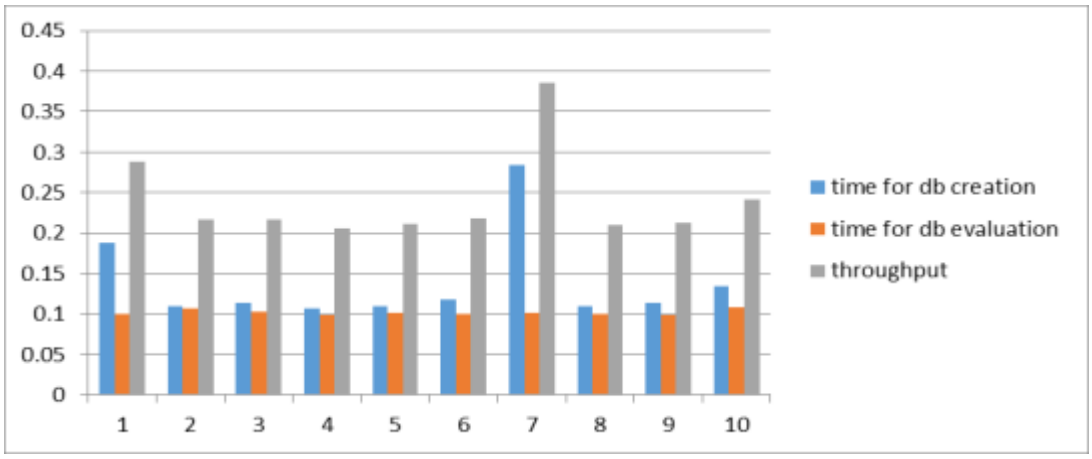

Fig 7. Performance of System

REFERENCES

1. R. Frischholz, U. Dieckmann,"BiolD: A multimodal biometric identification system", Computer, Vol. 33, No. 2, pp. 64-68,2000.
2. M. Golfarelli, D. Maio, and D. Maltoni, "On the error-reject tradeoff in biometric verification systems," *IEEE Trans. on Patt. Anal. and Mach. Intell.*, vol. 19, pp. 786–796, July 1997.
3. A. Ross and A. K. Jain, "Information fusion in biometrics," *Pattern Recognition Letters*, vol. 24, pp. 2115–2125, Sep 2003.
4. L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, "Is independence good for combining classifiers?," in *Proc. of Int'l Conf. on Pattern Recognition (ICPR)*, vol. 2, (Barcelona, Spain), pp. 168–171, 2000.
5. M. Indovina, U. Uludag, R. Snelick, A. Mink, and A. Jain, "Multimodal Biometric Authentication Methods: A COTS Approach,"
6. S. Arun Vivek, J. Aravinth, S. Valarmathy Professor "Feature Extraction for Multimodal Biometric and Study of Fusion Using Gaussian Mixture Model".