Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 6, June 2019, pg.89 – 94

Multi Biometric Recognition System

Sahana J S[1]; Tarun R R[2]; Manjunath C R[3]
*Department of CSE, School of Engineering and Technology-Jain University, Bangalore, India
[1] sahanajs97@gmail.com; [2] rrtarun04@gmail.com; [3] manjucr123@gmail.com

Abstract*— As there is a rapid increase in technology development increase in identity theft, consumer fraud, threat to personal data also increasing day by day. The methods developed earlier to secure personal information from theft were not efficient and safe. Biometrics were introduced when there was a need of technology to secure personal information more efficiently. The old fashioned traditional approaches such as Personal Identification Number(PIN), passwords, keys, login id can be forgotten, stolen or lost. In biometric authentication system, a user does not need to remember any passwords or carry any keys. Like humans recognize each other by physical appearance and behavioural characteristics biometric systems makes use of physical characteristics like fingerprints, facial recognition, iris recognition to distinguish between a genuine user and an impostor. Initially biometric identification methods were developed to enhance security in government and corporate sectors, but nowadays it has made its way to almost all the private sectors like Banking. Finance, Home safety and security, Healthcare, Commercial safety and security etc. Since biometrics samples and templates of a biometric system which has single biometric feature to recognize a user can be replaced and duplicated, a new idea of fusion of multiple biometric identification technology has been introduced called multi modal biometric recognition systems which makes use of two or more biometric characteristics of an individual to identify as a genuine user or not.

Keywords— Unimodal, Multimodal, Biometrics, Security, Accuracy

I. INTRODUCTION

In today's busy world, security is a major concern and everyone will look for reliable ways to ensure safety. The old ways of securing our homes and belongings was using key and lock systems which is quite inefficient as keys can be duplicated. Later the next level of protection was provided by modern technologies with PIN and passwords. Modern systems are quite efficient but it can also be hacked and gain access. In order to achieve high accuracy and reliability, Biometric Identification technology has been introduced which uses physical or behavioural characteristics to verify an individual. The main reason to choose biometric identification technology over traditional method of identification is that traditional identification techniques are vulnerable to security, not reliable and insecure. Majority of developed biometric systems use single biometric technology for identification and verification. These unimodal systems are unable to meet some of the challenges like enrolling large populations, high performance etc. Later an advanced biometric identification technology with better performance and high accuracy rate called multimodal biometric recognition system is being introduced. Multimodal systems are capable of using two or more physical or behavioural characteristics of humans to enroll, verify and provide decision. Multimodal biometric systems also combine two or more identification

technologies such as fingerprint systems and iris recognition systems with multiple sensors and provides decision by combining results from each subsystem. When using multimodal biometric systems if one sensor or system fails to perform identification the other systems can be used to make decision. Multimodal systems can be used in various areas such as in homes for biometric based door locks to prevent theft, in hospitals to record patients details, in software companies and educational institutions to maintain attendance, in banks for secure and safe processing of payment, biometric alarm systems in case of data security in various sectors. Multimodal systems are more advantageous and overcomes all the limitations of unimodal systems with increased security, high accuracy and liveliness.

II. RELATED WORK

In recent years, a lot of work has been carried out on different types of biometric identification techniques and their working, advantages and working of multimodal biometrics over unimodal and traditional approaches. [3] Biometrics refers to an automatic authentication of a person based on his physiological and behavioural characteristics. The usage of biometrics as a reliable means of authentication is emerging in almost all the government and private sectors. Some limitations of the unimodal biometric systems can be reduced by using multimodal biometric systems, which integrate information at various levels to improve performance. [4] In this paper they have proposed a new multi-modal biometric recognition system with fusion of fingerprint and iris recognition to achieve higher accuracy. The main aim of this paper is to show that the fusion of unrelated, independent identification techniques achieves better accuracy than any unimodal biometric systems. The output scores from two different systems are combined into single score at score level using three normalization methods and four fusion approaches. They have also used normalization steps to transform the unrelated, distinct scores into common scale from two techniques. In this paper they have briefed about types of fusion level in biometric systems. Sensor level, feature level, score level are the types of fusion levels. The first step at score level is score normalization where the scores are transformed into common format. The second step of fusion level has two categories like classification and combination. Classification approach classifies the decision into impostor or genuine. Combination approach combines the multiple decision score into single comparison score. The accuracy achieved by this work is more than 60%.

[5] By this paper we could understand that rank level fusion may be a comparatively new fusion approach. Fusion is done at the rank level, when the output of each biometric system was a subset of possible matches sorted in decreasing order of confidence. The intent of rank level fusion was to combine the output by individual biometric sub systems in order to achieve more accuracy. They have used face recognition, ear recognition and signature recognition systems and processed those using Eigen face projection and Fisher face projection for face enrolment and identification, Eigen ear projection for ear enrolment and identification and Eigen signature projection for signature enrolment and identification. So through feature matching based on the ranks of face, ear and signature the rank level fusion happened and final output was gained by them. By their experiment they came into a conclusion that fisher face worked more efficiently than the eigen face technique and out of the three biometric recognition systems eigen face worked or performed better than the eigen ear and eigen signature.

[6] This paper presented the related works and performance analysis for fingerprint biometric. The assessment of performance is done on reviewed works using various specifications and available methods. The various issues related to unimodal biometric systems is discussed in this paper [7]. The security and privacy concerns that biometric authentication raises need to be addressed. [6] It is surveyed that automatic fingerprint recognition is the best candidate biometric technology for explosives security from an analysis of the requirements: security, usability, ruggedness, size, form factor, privacy and operational temperature range. [2] In this paper they have showed that if either of the two biometric systems work then the person could be successfully recognized. So they collected the samples of fingerprints and iris, these were extracted and compared in their system. Finger prints were enhanced and went their minutiae extraction and if the matching with fingerprint database took place then the person was recognized or if not recognized then the person had to undergo another set of identification test that was iris identification. The iris was pre-processed and then followed by extraction of features then if it matched with the iris database then the person was identified or the person was not identified. Based on their experiment for fingerprint recognition, if they gave small thresholds

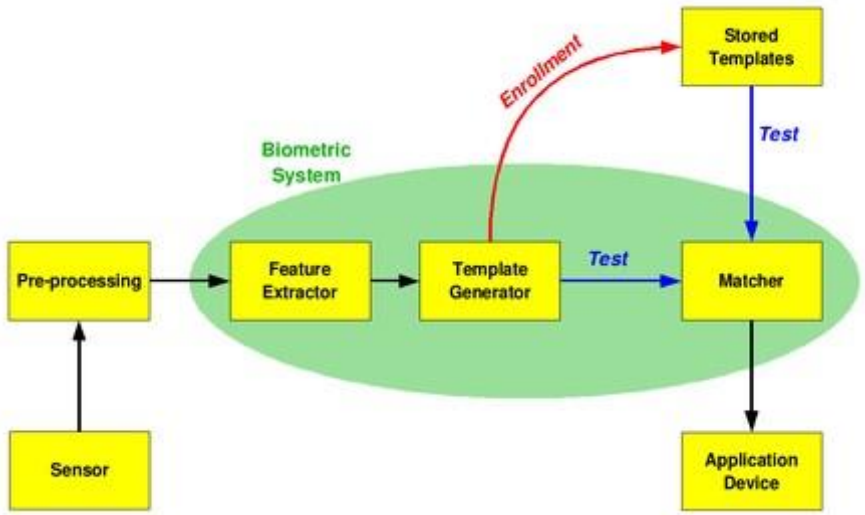
then acceptance of wrong fingerprints was higher and the accuracy decreased when compared to higher threshold where accuracy increased along with lower acceptance of wrong fingerprints. For iris recognition they had used hamming distance. The accuracy was more for iris recognition as compared to fingerprint recognition. [1] In this paper, they have considered fingerprint extraction and evaluation and also finger vein extraction and conversion to recognize a person. The have also fused the two biometric recognition systems using Enhanced partial discrete Fourier transform (EP-DFT) as the DFT matrix has its own features such as orthogonality. As DFT matrix reduces the time to multiply it with a matrix so the partial Discrete Fourier Transform became compact and computationally efficient. They have considered three different fusion options where they have considered minutia-based fingerprint feature set and image-based finger-vein feature set using a feature level fusion strategy. By their analysis they concluded that EP-DFT greatly enhanced system security compared with the original P-DFT. They also concluded that it is imperative to design good, efficient non-invertible transformation functions for cancellable multi-biometric systems.

III. PROPOSED APPROACH

Single or unimodal biometric systems are not sufficient enough to recognize a person efficiently so we propose multi biometric system for authentication to achieve better security and reliability. We are particularly focusing on usage and rate of accuracy achieved by multi biometric recognition systems in home security and various areas. We shall explore more about multi biometric recognition systems in various fields.

METHODOLOGY

The following steps are the procedures followed while identifying an individual.



1.Enrollment of the biometric samples of a candidate

Enrolment is when a candidate uses biometric system for the first time, a sample biometric trait like fingerprint or iris is captured and stored in a database for later comparison.

2.Obtain/Acquire Live Samples from Candidate

First obtain the biometric sample from the user using sensors.

3.Extract feature

Process and extract the prominent features from the captured sample.

4.Comparison of samples

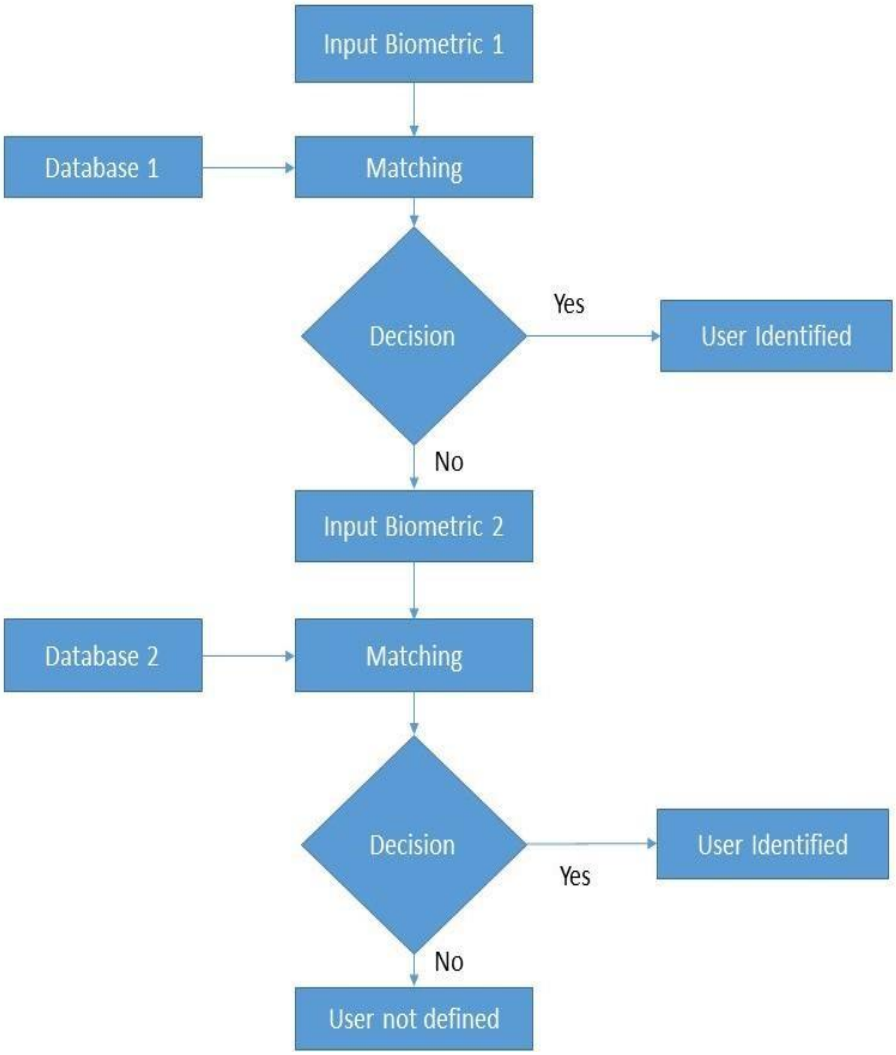
Compare the live samples captured with the all the samples stored in the database using algorithms.

5.Display decision

When input samples matches with the registered samples it will accept the candidate or rejects.

FLOW DIAGRAM

The below is the flow of working procedure of multi biometric recognition systems.



- At first, the sample biometric feature is captured from the user when a user wants access. The biometric feature can be fingerprints, palm prints, retina image, iris image etc.
- The captured biometrics are pre-processed which includes removal of unwanted data, noise, and a prominent feature is extracted on which a person is to recognised.
- The extracted feature is compared with enrolled samples which is stored in the database to make sure both the samples having similarities.
- The enrolled sample and the captured sample are compared in various angles using some defined algorithms and the matching accuracy is displayed.
- Based on the rate of accuracy the decision is made as genuine user or an imposter.
- If one biometric system provides 60% accuracy which is not adequate to make any decision, another system with another biometric feature is used perform the same procedure.
- The final results obtained from all the sub systems are scaled and transformed to common format and the decision is displayed on the screen.

Nowadays biometrics has become an emerging trend in public and private workspace where data or any personal security is the vital concern. Most of the peoples are moving from traditional way of securing their homes to technological way. Instead of lock and key system, multi biometric door locks are used which is a combined system of two or more biometric identification technique to verify and authenticate. Biometric door

will be having latch with fingerprint recognition or palm print recognition to identify owner of the house. A video door bells have been introduced which offers an easy way to check who is at the door without getting close to the door. Video door bells can be connected to your smart phones via Wi-Fi network and user can get an alert when someone approaches the door. The video doorbell records video when the doorbell is pressed and offers two-way audio communication that allows you to communicate with the visitor from anywhere via your phone. Other features include face recognition technology that identifies visitors by name, motion sensing technology that knows the difference between people, cars, and animals.

Biometrics are also used in many organizations and educational institutions to record employee's attendance. Multi biometric attendance system provides flexibility to employees to record their presence and working hours with proper time interval. The main advantage of using multimodal biometric systems is speedy identification and authentication. If one of the modality fails to identify and present decision a user can choose other modality or based on user's convenience, he/she can choose the modality to gain access. Biometrics are also used in financial sectors like banks, ATM's, Insurance companies for secured transactions. Financial sectors are very sensitive in terms of transactions because they may lose huge amount of money due to spoofing. In order to provide secured transactions financial sectors are adopting biometric identification techniques to identify account holders and also for KYC. Vein scans and iris scans are popular nowadays where a user does not require to contact sensor and it is more reliable and faster than other biometric technologies. Healthcare centres are also using biometrics to identify right patient, to secure patients medical history and treatment plan.

IV. CONCLUSION

In this digital era, most of the biometrics systems existing uses information from single biological feature for verification and identification. Due to vulnerability of biometric sensor to noisy or bad data the captured sample of the biometric feature might become false and there will be a chance of rejecting an enrolled user incorrectly and accepting a fake user falsely. In case of fingerprint recognition system, scanners might fail to recognize dirty or wounded fingers also underdeveloped fingerprint ridges in case of young children and faded fingerprint ridges in case of elders. Where as in case of facial recognition system, sensors may not be able to recognize identical twins whose appearance will be almost similar. Also in case of voice recognition systems a person can imitate some other person's voice and gain access to their personal information. In all the above cases due to false decision from the scanning devices an unauthorised person gains access and it leads to fraudulent activity. In order to overcome these problems a biometric system with fusion of two or more biological features and sensors called multi-biometric systems are used. The main advantage of using multimodal biometric recognition is improved authentication accuracy. So using multi-biometric recognition systems help us in identifying a person more accurately as compared to using a single biometric recognition system.

We have learnt about the various biometric recognition systems so we can use the necessary multi-modal biometrics for smart homes so that we can have a secure and reliable access to our homes. We can conclude that multi-modal biometrics are more reliable and accurate as compared to uni-modal biometric recognition systems.

REFERENCES

[1] Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng, Craig Valli, "A Fingerprint and Finger-vein Based Cancelable Multi-Biometric System", Pattern Recognition Volume 78, June 2018, Pages 242-251, 2018.

[2] Mohamed Elhoseny, Ahmed Elkhateb, Ahmed Sahlol and Aboul Ella Hassanien "Multimodal Biometric Personal Identification and Verification", Springer International Publishing AG 2018.

[3] A.H. Mir, S. Rubab, Z. A. Jhat, "Biometrics Verification: A Literature Survey", International Journal of Computing and ICT Research, Vol. 5, No.2, December 2011, Dept. of Electronics & Communication Engineering, Dept. of Physics, Dept. of Electronics, National Institute of Technology, Hazratbal, Srinagar, J&K.

[4] Kamer Vishi, Sule Yildirim Yayilgan, "Multimodal Biometric Authentication using Fingerprint and Iris Recognition in Identity Management", 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Faculty of Computer Science and Media Technology, Dept. of Information Security Gjøvik University College.

[5] Md. Maruf Monwar, "Multimodal Biometric System Using Rank-Level Fusion Approach", IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, Vol. 39, No. 4, August 2009, Student Member, IEEE, and Marina L. Gavrilova, Member, IEEE.

[6] Ravi Subban and Dattatreya P. Mankame, "A Study of Biometric Approach Using Fingerprint Recognition", Lecture Notes on Software Engineering, Vol. 1, No. 2, May 2013.

[7] Mohamed Soltane and Mimen Bakhti, "Multi-Modal Biometric Authentications: Concept Issues and Applications Strategies" International Journal of Advanced Science and Technology Vol. 48, November, 2012, Electrical Engineering & Computing Department, Faculty of Sciences & Technology Doctor Yahia Fares University of MEDEA, 26000 MEDEA, Algeria.

[8] Brahim Omar, Gang Xiao, Moussa Amrania, Zifei Yane, and Wangmeng Zuo, "Deep Features for Efficient Multi-Biometric Recognition with Face and Ear Images", Ninth International Conference on Digital Image Processing (ICDIP 2017), 2017

[9] Lu Leng, Ming Li, Cheonshik Kim, "Dual-source discrimination power analysis for multi instance contactless palmprint recognition", Multimedia Tools and Applications, Volume 76, Issue 1, pp 333–354, January, 2017.

[10] Ghassem Mokhtari, Qing Zhang, Chad Hargrave, Jonathon C. Ralston, "Non-Wearable UWB Sensor for Human Identification in Smart Home", IEEE Sensors Journal, Volume: 17, Issue: 11, June1, 2017.

