Multimodal Biometric Identification for accessing Personal vault based on IoT Security System

[1]Mrs.S.Arunarani M.C.A.,M.Phil.,NET.,SET., [2]Dr.Gobinath Ramar
[1] Research Scholar, Department of Computer Science, Vels University, Chennai.
Assistant professor, Prince Shri Venkateshwara Arts and Science College, Chennai.
[2]Assistant Professor, Department of Computer Science, Vels University, Chennai.

Abstract: In the Internet of Things (IoT), identification of an object is the pivotal technology for authentication, to control access, and to fabricate assurance between object and process. In pattern recognition technologies, face and fingerprint are used for secured identification and authentication. Face and Fingerprint inputs are given by user from his mobile or any device to control process using Internet of things (IoT). In control process, identifications take place by fusing the inputs and then pass the decision signal to automatically open the vault. In this paper, we propose a face and fingerprint identification and authentication scheme based on PCA to solve the problem. The face and fingerprint of user is enrolled to introduce the processes of face and fingerprint identifier generation and matching. Then, parallel matching mechanism is proposed to efficiently resolve face and fingerprint image, control personal data access and confirm user's identity information. It makes full use of the advantages of IoT to effectively improve computation power and storage capacity. The proposed scheme is practically feasible and can provide efficient face and fingerprint identification and authentication service. Improved efficiency is achieved by integrating multiple modalities in user identification and authentication.

Keywords:- Internet of Things and biometrics - face - fingerprint – multimodal- security-authentication.

1 Introduction

Human physiological or behavior characteristics can be used as a biometric to authorize the identity of an individual. Any biometric system for authentication operates in two approaches: Enrollment and Authentication. In the enrollment mode, using a biometric sensor the required biometric of the user is obtained and stored in a database. The acquired biometric sample is named with a user identity to promote authentication. In the authentication mode, biometric data from the user is obtained and used to verify the identification of the user or to identify who the user is. Verification is a process where it compares the user's biometric with those templates analogous to the claimed identity. Identification involves comparing the obtained biometric data against the samples of all users in the database. Biometric assure greater security to our data than password as this system use the biological characteristics of a person to examine their identity. Some of the biometrics that can be used is fingerprint, face, iris, voice, signature, hand geometry, hand vein, retinal pattern, ear, facial thermo grams, odor, gait and DNA.

Unimodal Biometric systems are often not able to meet the required performance because of its various problems such as noisy data, intra-class variations, confined degree of freedom, non-university, spoof attacks and high error rates. These limitations can be overcome by using multimodal biometric systems that combine the biometric data from multiple sensors. In multimodal biometrics, it integrates two or more biometric modalities for a authentication/identification system. Identification based on multiple biometrics increase the recognition rate.

Internet of Things (IoT)

Internet of Things (IoT) is a collection of digital machines, devices, biometric characteristics and mechanical devices. The IoT permit exchange of data with different objects which make decisions themselves and also remote management.

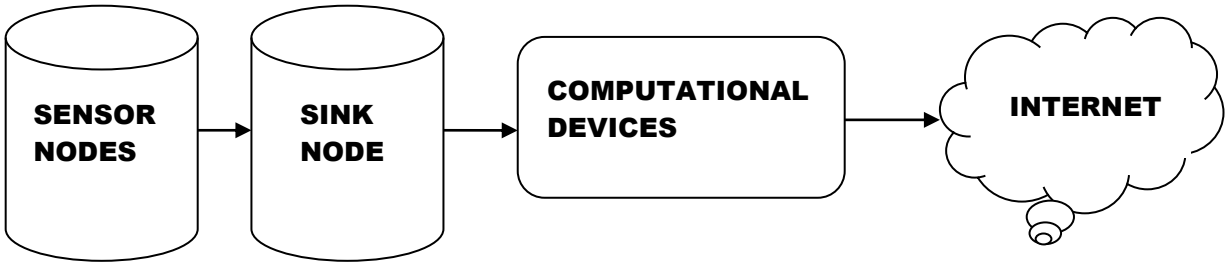
Global market is taken by the IoT technology through digital transformation of computing and communication development. With these technologies interconnected among universal things for the given applications and services are rendered by both physical-space and cyber-space. Various physical objects such as human, sensors, computers, mobile devices etc., are used to access internet as building blocks of IoT and enable applications, in physical space. In the cyber space, the generated objects are used for identification. As an essential part of IoT, identification and resolution technology has been enforced in various IoT schemes. For example, access protector, logistics, food safety, supply chain management, Finance using internet, mobile payments, etc. Authentication of physical object has become a valuable research subject for object authentication, data access process.

Five domains [2] of the IoT to communicate with each other in different environments are:
• Transportation and strategy domains (Logistics, Assisted driving, Mobile ticketing, Environment monitoring),
• Healthcare territory (Tracking, Identification/ Authentication, Data collection, Sensing),
• Smart environment (Comfortable homes/offices, Industrial plants, Smart museum and gym),
• Personal and social domain (Social networking, Historical queries, Losses, Thefts),
• Futuristic scope (Robot taxi, City information model, Enhanced game room).

2. Architecture Outline To Secure Io Using Multimodal Biometric System

Securing personal data is very essential and fundamental process which uses the Internet of Things. One of the ways is to plan and design a biometric system. The given figure 1 shows how to biometric system secures the Internet of Things. First biometric system performs feature extraction from the user's unique biometric trait and it is verified. If the verification is positive, the information from the user is collected and it is send to computational device from sink node. Then the processed data is stored in the internet of things for sharing and processing. Different addendum is possible by adding more sensor nodes, by using various biometric traits for authentication and identification between different users.

Fig.1: Architectural outline



Eventually, facilitated by cloud IoT and IoP will be interconnected to each other. The human identification for identity authentication, for data access and for privacy of information will become more valuable research.

Face and fingerprint biometric authentication technique is more effective to improve the security. The existing biometric identification techniques are unimodal biometric identification and multimodal biometric identification with two complete unimodal systems. Unimodal biometric system consists of its own unique feature extractor and classifier. Its reliability is decreased because it requires memory footprint, less accuracy, and it has slower processing speed.

3. Face Biometric Concept

Face is a biometric which is very reliable and unique for human identification. In face identification process, the facial images are analyzed and pixels and feature points are extracted from the size and position of eyes, nose and mouth. Conclusively, using the extracted facial feature value, individual is identified based on face identifier application service.

Face identification system use about 80 different features in our faces and those are referred as nodal points. In some cases unique features like scar or mole are also added as features.

Advantages of face as biometric are

*Simple camera is enough to capture the image which results in low cost hardware.

*it can be used without the person's knowledge that he or she is identified.

Disadvantages of facial biometric are

- Facial features differ with age and disease.
- Required features cannot be captured if the person wears hat, glass etc.,

The face recognition system involves two phases: face identification and face resolution. The functional modules and methods are same in both the phases. They are as follows:

- Image acquisition and detection:
  In this module facial image of the user is captured using any camera and only the facial region used for face identification is obtained by removing the useless regions.
- Preprocessing of the image
  Sometimes the quality of the facial image is not obtained to the required standard, so preprocessing operations such as thinning, graying, normalization are done to enhance the image.
- Feature extraction and matching:
  Using some feature extraction algorithm, facial features are extracted and compared with all the enrolled facial features stored in the database. According to the matching module, it includes two results: identity is confirmed or it is unidentified.

4. Fingerprint Biometric Concept

Fingerprint is one of the oldest and internationally accepted biometric to identify a person. Fingerprint is the thumb impression of a person. Fingerprint is unique and rigid. Fingerprint is used in various applications such as defence, forensics, license registration, education, law, mobile log-in, etc,. Now-a-days, fingerprint sensors are based on thermal, optical, silicon and ultrasonic methods are available. Fingerprint recognition is based on minutiae and direction of the ridge endings and bifurcations

along a ridge path. Fingerprint matching is based on two techniques: minutiae-based matching and pattern based matching. In Minutiae matching, location and direction of each nodal points are used for identification. In pattern matching, two images are compared for similarity.

Advantages of fingerprint biometric are summarized below:

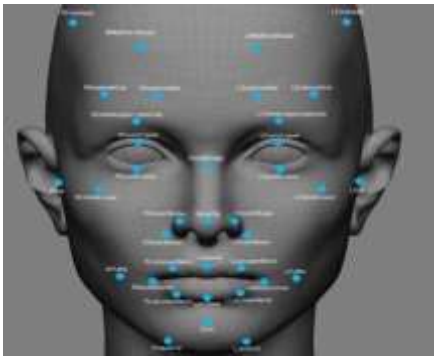
- Fingerprint is permanent for the whole lifespan of a human.
- Fingerprints establish high level of uniqueness.
- Fingerprint sensors are cost effective.

For perfect fingerprint recognition, three main steps are involved. They are

1. Fingerprint Pre-processing 2. Feature extraction 3. Fingerprint Matching

Pre-processing is an important step for enhancing the quality of the image. Feature extraction step involves thinning of the image, and extracting the features of the image. Fingerprint matching involves matching the enrolled image with the input image. This step determines whether the two fingerprint images are same finger or not.

Fig.2: face and fingerprint biometric



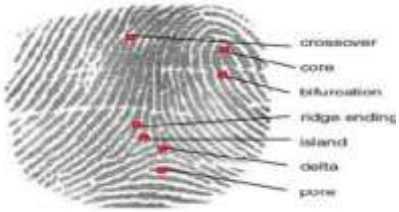
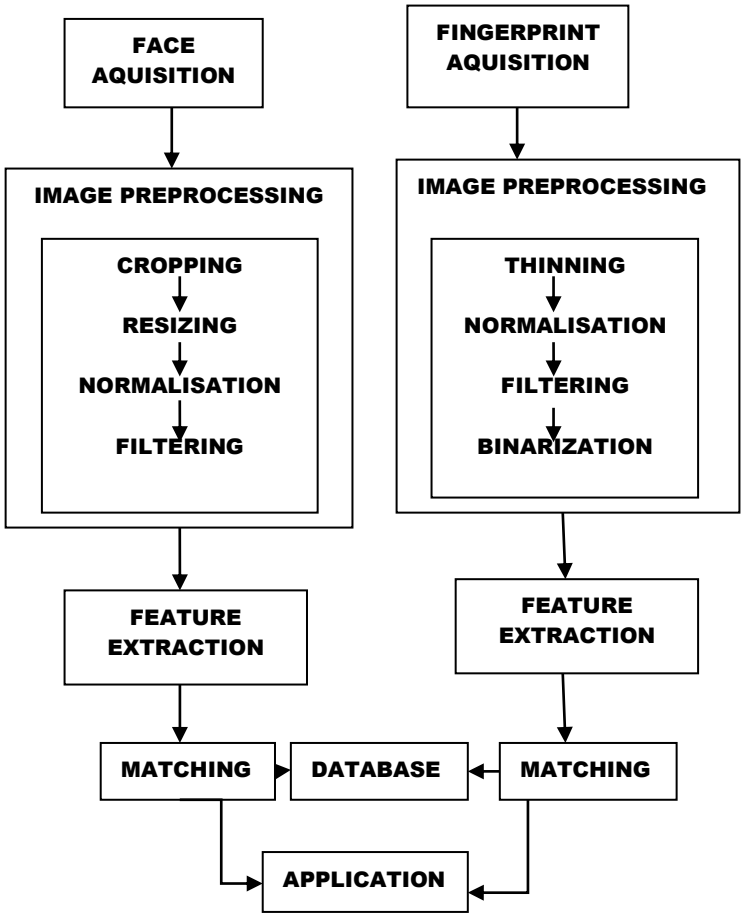


Figure given below explain the fusion of both the biometric for calculating the score value and if the score value is maximum then the user is identified as authorized and if the score level is lower than the threshold then the user is unauthorized.

Fig. 3: Multimodal biometric fusion

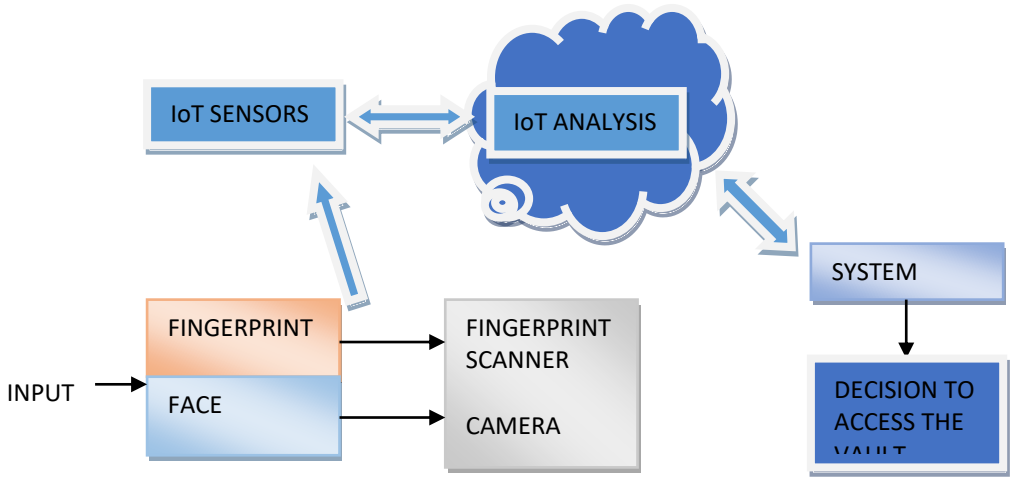


5. Proposed Methodology

In the proposed plan automated security to the personal vault using fusion based multimodal biometric identification system. In this method, face and fingerprint are used as biometric database. Two biometric traits are fused to decrease the possibility of hacking. The basis behind the proposed system is schematically represented in Fig. 4.

The input is given to the cyberspace by the user through his/her device. Verification of both the inputs i.e.,face and fingerprint are done in cyberspace. After the verification of the details about the user, the system passes on the signal for the vault to open.

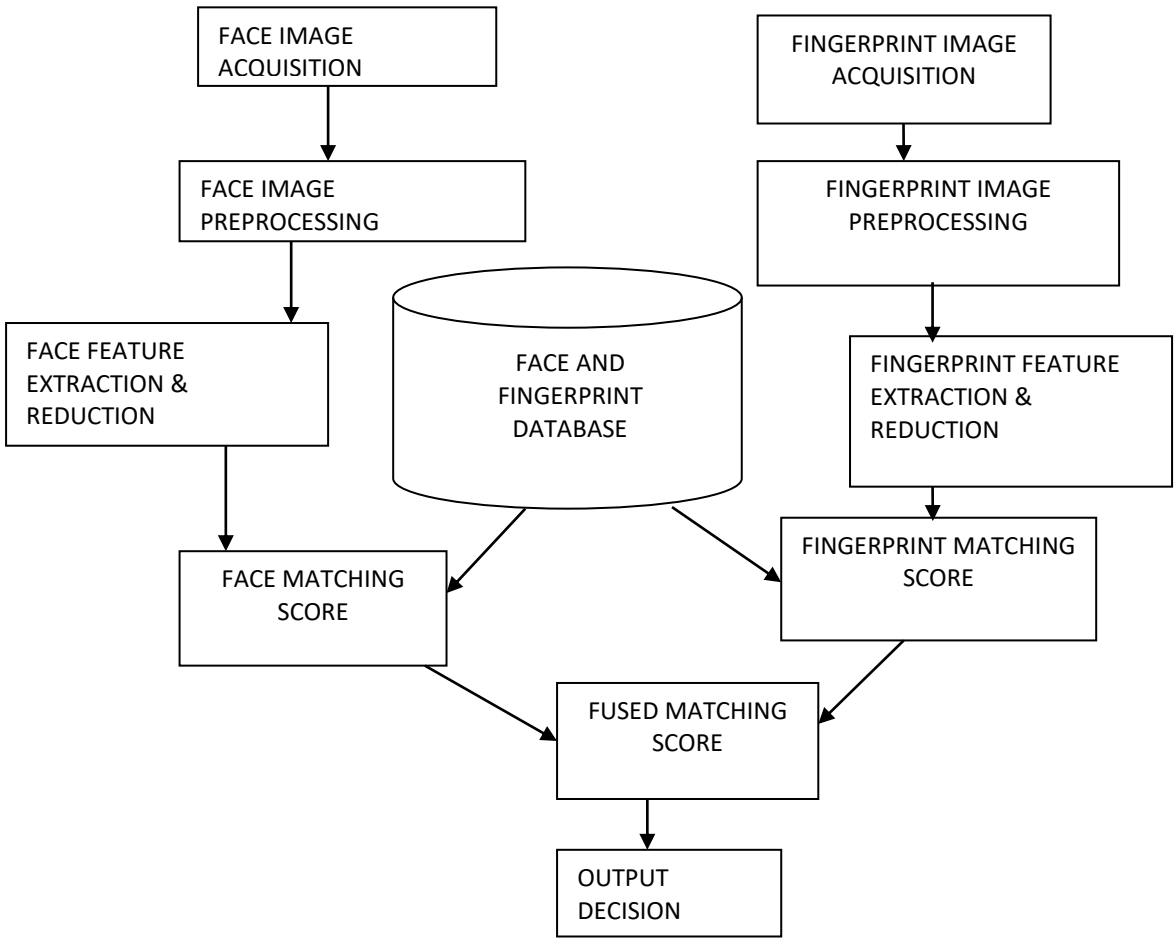
Fig. 4 proposed method



The proposed plan is better than the existing methodologies by giving higher security. The block diagram for the proposed methodology is shown in Fig. 4.

Basically, the first input from the user, i.e., fingerprint is captured and approved by the matcher, then the second input i.e., face of the user is obtained and verified by the matcher. The process gets completed after the fusion of both the biometrics. The proposed fusion based multimodal biometric is shown in fig.5.The proposed plan use simple design, improved processing speed, high security, use less memory which increase the effectiveness of the system.

Fig. 5Proposed multimodal biometric methodology



6. Result And Discussion

Fusion score value will say about the identification of user. Here one fingerprint and face images are selected from the input database and it is matched against the entire enrolled database of images. The user is identified as an authenticated person to open the vault only if the given input equated with the enrolled database. If the given input is not equated then the user is not allowed to open the vault as he/she is identified as unauthorized person. When the proposed method is compared with the existing method, it is clear that the proposed method show an improved efficiency in the recognition rate.

7. Conclusion

In this paper, the concept of combining the characteristics of face and fingerprint make us establish very high efficiency and performance. The vital advantage of this multimodal biometric authentication is low cost hardware and software is used and very small memory is used for implementation. The proposed plan can be used in areas where we want high security like migration checking, defence and internet payment. This paper explains a methodology which is computationally low cost and use very low storage space. This method needs only a high quality camera which is present in all the smartphone and with that any user can identify them with one image. Future work will be focused on adding more security measures and using biometrics which preserve privacy of the user.

References

1. Sujatha, K., Pappa, N.: Combustion monitoring of a water tube boiler using a discriminant radial basis network. ISA Trans. 50, 101–110 (2011)
2. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey.Computer networks, 54(15), 2787-2805.
3. Jain, A.K., Hong, L., Kulkarni, Y.: A multimodal biometric system using finger prints, face and speech. In: 2nd International Conference Audio and Video-based Biometric Person Authentication, pp.182–187. Washington, March 22–24 (1999)
4. Jain, A.k., Prabhakar, S., Chen, S.: Combing multiple matchers for a high security fingerprint verification system. 20(11–13), 1371–1379 (1999)
5. Roli, F., Kittler, J., Fumera, G., Muntoni, D.: An experimental comparison of classifier fusion rules for multimodal personal identity verification system, pp. 76–82 (2002)
6. Lumini, A., Nanni, L.: When fingerprints are combined with iris—a case study: FVC2004 and CASIA. Inter. J. Net. Sec. 4, 27–34 (Jan 2007)
7. Nandakumar, K.: MultiBiometric systems: fusion strategies and template security. Ph.D. Thesis, Michigan State University (2008)
8. Masek, L., Kovesi, P.: MATLAB source code for a biometric identification system based on iris patterns. The School of Computer Science and Software Engineering, the University of Western Australia (2003)
9. Maček, Nemanja & Franc, Igor & Bogdanoski, Mitko & Mirković, Aleksandar. (2016). Multimodal Biometric Authentication in IoT: Single Camera Case Study.
10. Entertech, "Biometrics to Secure the Internet of Things", Dec. 9, 2015. Last time visited: August 20, 2016.
11. Sujatha K., Ponmagal R.S., Senthil Kumar K., Shoba Rani R., Dilip G. (2018) IoT-Based Multimodal Biometric Identification for Automation Railway Engine Pilot Security System. In: Satapathy S., Bhateja V., Das S. (eds) Smart Computing and Informatics. Smart Innovation, Systems and Technologies, vol 77. Springer, Singapore
12. P. Hu, H. Ning, T. Qiu, Y. Xu, X. Luo, A.K. Sangaiah, A unified face identification and resolution scheme using cloud computing in internet of things, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.03.030
13. R. Rouhi, M. Amiri, B. Irannejad, "A Review on Feature Extraction Techniques in Face Recognition", Signal & Image Processing: An International Journal (SIPIJ) Vol. 3, No. 6, pp 1-14, 2012.
14. International Telecommunication Union, "Overview of the Internet of things," Recommendation ITU-T Y.2060, June 15, 2012.

15. A. K. Jain, A. Ross, "Introduction to Biometrics", In "Handbook of Biometrics", A. Jain et al. (Eds), Springer,2008.
16. C. Perera, R. Ranjan, L. Wang, Lizhe, S. Khan, A. Zomaya, "Privacy of Big Data in the Internet of Things Era", EEE IT Special Issue Internet of Anything, 6., 2015.
17. P. Balakumar, R. Venkatesan, "A Survey on Biometrics based Cryptographic Key Generation Schemes", International Journal of Computer Science and Information Technology & Security, Vol. 2, No. 1, pp. 80-85, 2012.
18. Multimodal Biometric Authentication in IoT: Single Camera Case Study The Eighth International Conference on Business Information Security (BISEC-2016), 15th October 2016, Belgrade, Serbi NEMANJA MAČEK, IGOR FRANC, MITKO BOGDANOSKI,ALEKSANDAR MIRKOVIĆ