IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114122

Literature Review :- Multimodal Biometric Authentication System

Anand Sagar[1], Hiralben Ganeshbhai Patel[2], Navneetkumar Maurya[3]

Dr. D.Y Patil School of Engineering Academy

Abstract: The Unimodal biometrics has many problems such as noisy data, intra-class variations, confined degrees of freedom, non uniformity, spoof attacks, uniqueness and diverseness, non invariant and spoofy attack. The use of single property works as exclusive source of information for authentication (e.g. fingerprint, face, voice, gait etc.) generally leads to high false acceptance rate (FAR) and false rejection rate (FRR), Failure to Enroll rate (FER). . In order to conquered the limitations provided by unimodal system there is need of system which can combine of two or more attributes types of biometrics systems known as multimodal biometric systems. These systems are more authentic and trustworthy due to the presence of multiple, self contained, individualistic biometrics attributes. The spoofing problem is solved easily because it is very difficult for deceiver to take-off multiple biometric traits. The advantages of multimodal biometric systems are that there are multiple sources of information. As multimodal biometric systems use more than one biometric trait so it provide more security and more reliable and provide maximum accuracy.

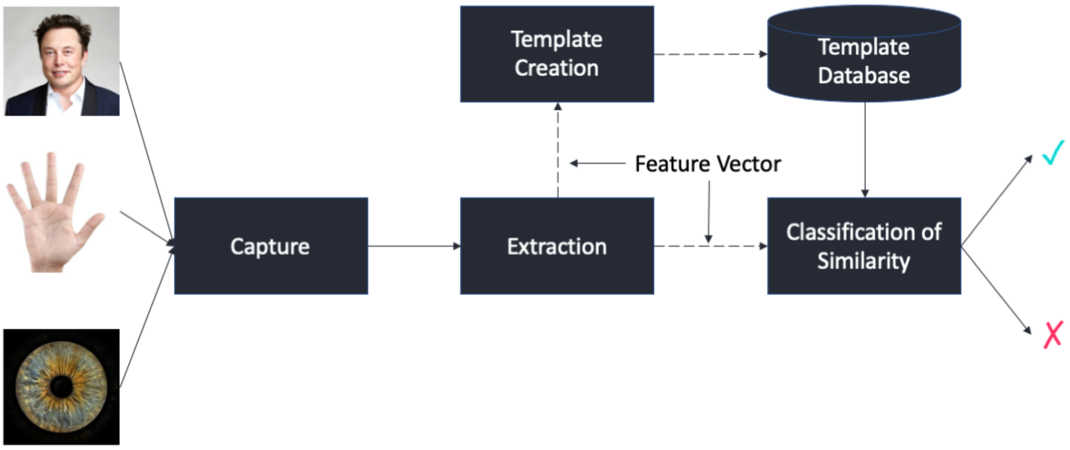
INTRODUCTION:

The term Biometric made with two terms Bio means life and metrics means to measure. Biometric authentication system are becoming popular due to increased security and proven its superior performance due to increasing demand in society. It uses measurable human physiological or behavioral characteristics to verify identity of individual and has the ability to distinguish between an authorized person and fake ones. Biometric system improved the recognition technique by determining the physiological, behavioural traits. Physiological characteristics which remain constant lifetime include fingerprint, face, DNA, iris etc. and each of these properties are remarkable to every person. Behavioral traits are signature, voice; speech patterns, gait, keystroke etc which amend with time due to age, disease, fractured, accident and several other things affect behavior. Biometric features are unique for every individual so cannot be forgotten by users and outperforms technology. Even though it used in every field like in forensic, commercial, medical, financial institution, border security, and so on but has its drawbacks in terms of cost, accuracy, throughput and ease of use. Biometrics based on single peculiarity is known as unimodal system with a variety of problems like noisy data, false rejection, intra class variation, fake biometric trait, non universality, inter-class similarity, spoofy attacks. To overwhelm these problems multimodal biometrics is used. In multimodal different cues or traits are collected from different sources of same person.

MULTIMODAL BIOMETRIC AUTHENTICATION

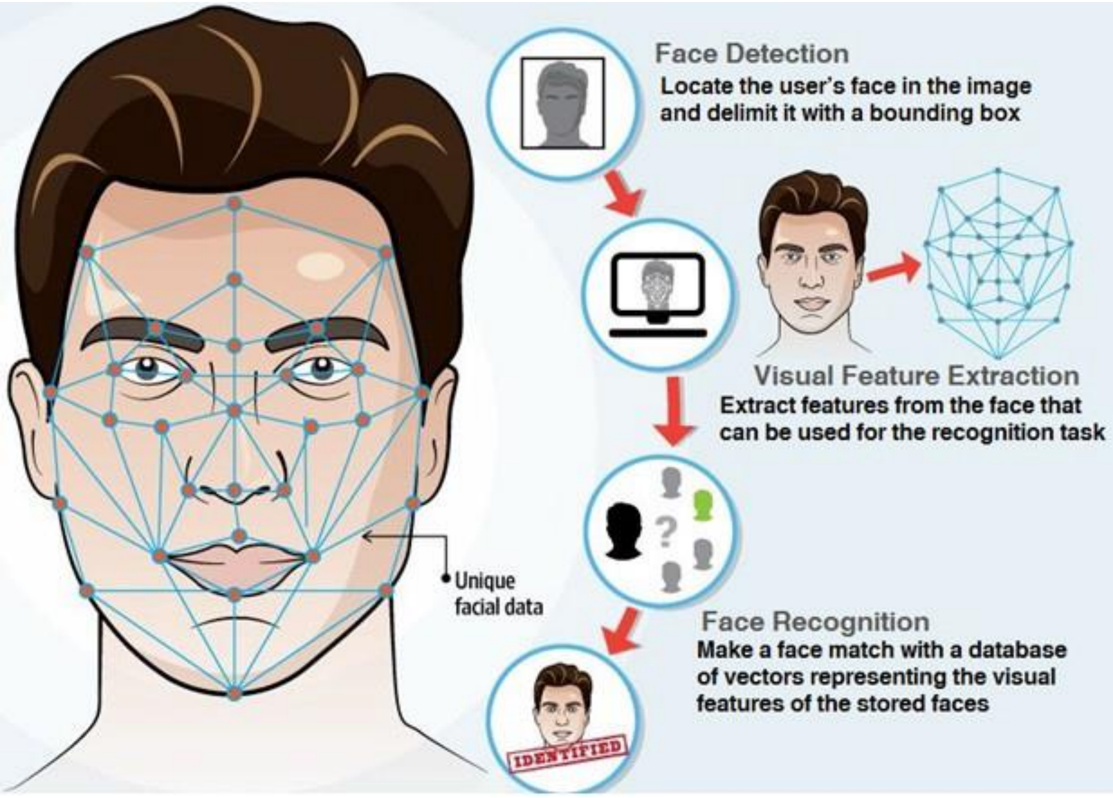
With computers and security, biometrics is the identification of a person by the measurement of their biological features. For example, users identifying themselves to a computer or building by their fingerprint or face is considered a biometrics identification. Compared to a password, this type of system is much more difficult to fake since it is unique to the person. Other common methods of a biometrics scan are a person's voice, hand, iris, and retina. **Multimodal biometric is the usage of multiple biometric indicators by personal identification systems for identifying the individuals. Multimodal authentication provides more level of authentication than unimodal biometrics which uses only one biometric data such as fingerprint or face or palm print or iris. In computer science, in particular biometrics is used as a form of identity access management and access control. By using biometrics it is possible to establish n identity based on who you are such as ID cards.** Biometric login **provides a convenient method for authorizing access to private content within your app**. Instead of having to remember an account username and password every time they open your app, users can just use their biometric credentials to confirm their presence and authorize access to the private content.

DOI: 10.17148/IJARCCE.2022.114122



FACIAL RECOGNITION

A facial recognition system is a technology capable of matching a human face from a digital image or a video frame against a database of faces, typically employed to authenticate users through ID verification services, works by pinpointing and measuring facial features from a given image. Facial recognition systems are employed throughout the world today by governments and private companies. Their effectiveness varies, and some systems have previously been scrapped because of their ineffectiveness.


Face Detection
Locate the user's face in the image and delimit it with a bounding box
Visual Feature Extraction
Extract features from the face that can be used for the recognition task
Face Recognition
Make a face match with a database of vectors representing the visual features of the stored faces
Unique facial data
IDENTIFIED

FINGERPRINT RECOGNITION:

Fingerprint recognition allows a person to be verified or identified through the analysis and comparison of his or her finger dermal ridges. Fingerprint recognition was one of the first techniques used for automatically identifying people and today is still one of the most popular and effective biometric techniques

Block diagram of fingerprint process system.

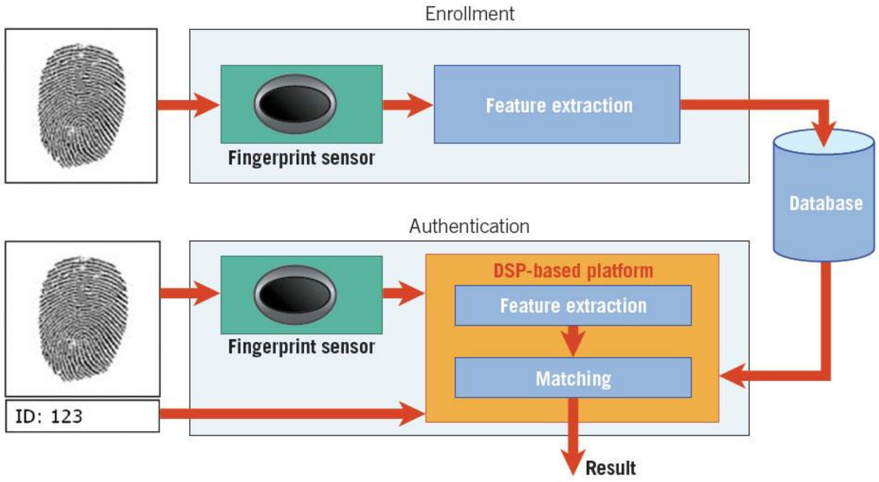


Figure 1

CONCLUSION:

Now a day's biometric systems are widely used to overcome the problems of traditional authentication. **Face recognition is an emerging technology that can provide many benefits**. Face recognition can save resources and time, and even generate new income streams, for companies that implement it right. Each fingerprint examination will result in one of the following conclusions: The fingerprint was made by (identified/individualized to) a known source (victim, suspect, etc.) The fingerprint was not made by (excluded to) a known source. The fingerprint cannot be identified or excluded to a known source (inconclusive).

REFERENCES:

1.L. Hong, A. Jain and S. Pankanti, "Can Multibiometrics Improve performance", Proceedings of AutoID 99, pp. 59-64, 1999

2.A. Ross and A.K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, vol. 24, no. 13, pp. 2115-2125, 2003.

3.A.S. Tolba and A. A. Rezq, "Combined Classifier for Invariant Face Recognition", Pattern Analysis and Applications, vol. 3, no. 4, pp. 289-302, 2000.

4.Anil K. Jain and Jianjiang Feng, "Latest Fingerprint Matching", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 33, no. 1, Jan 2011.

6.W. Yunhong, T. Tan and A.K. Jain, "Combining Face and Iris Biometrics for Identity Verification", Proceedings of Fourth International Conference on AVBPA, pp. 805-813, 2003.

7.S.C. Dass, K. Nandakumar and A.K. Jain, "A Principled Approach to Score Level Fusion in Multimodal Biometric Systems", Proc. of Audio- and Video-based Biometric Person Authentication (AVBPA), 2005.

8.AK Jain and U. Uludag, "Hiding biometric data", IEEE Trans. Pattern Anal. Machine Intel., vol. 25, no. 11, pp. 1498-5, 2003.