A STUDY ON DEVELOPMENT OF A BIOMETRIC AUTHENTICATION SYSTEM

Dr. Rahul Kumar Budania
Assistant professor
Electronics & Communication Engineering
Shri JJT University, Jhunjhunu, Rajasthan
rahulbudania93@gmail.com

ABSTRACT

This study covers the field of biometric systems focus on biometric authentication systems. A short and general overview of biometric authentication systems gives some insight in how the various biometric data can be used for authentication. The problems of varying biometric data, caused by noise respectively human nature and approaches to solve these problems with multi-biometric systems in combination with information fusion, are also discussed. Since there is such a vast range of variances for the usage of biometric systems, some type of statistics is determined. Biometrics is the measurement of biological data. The term biometrics is commonly used today to refer to the authentication of a person by analyzing physical characteristics, such as fingerprints, or behavioral characteristics, such as signatures. Since many physical and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems. The word biometrics comes from two Greek words and means life measure. To provide a comprehensive survey, we not only categorize existing biometric techniques but also present detailed of representative methods within each category. Physical characteristics commonly used in biometric authentication include face, fingerprints, handprints, eyes, and voice. Another program compares this pattern with the one representing the user that was recorded earlier and stored in the system database.

Keywords: *Biometric authentication, biometric systems, fingerprints, handprints, eyes, and voice, computer networks, database, ID cards, keys, passwords.*

INTRODUCTION

Biometric systems are increasingly being adopted to improve security, convenience, and inclusion in society and to provide potential applications in various research and industrial fields. Notable biometric traits that have been successfully used in practical applications include the face, fingerprint, and iris. Furthermore, the recent advancement of artificial intelligent technologies makes them vulnerable to spoofing attacks (or presentation) through their inherent weakness. A common spoofing attack on faces or fingerprints was explored and discussed. In order to combat against presentation attacks and illegitimate user access to the systems, aliveness detection or continuous biometric authentication approaches should be taken into account. Continuous biometric authentications continuously check the identity of the user by using non-invasive measurable sensor that can collect users' biometric data. Thus, continuous biometric authentication has gained a lot of attention as a next-generation promising technique due to unique characteristics of the electrocardiogram (ECG) signals; it may be very promising trait mechanism for continuous biometric authentication. Since the liveness nature of ECG signals is not only ubiquitous and easy to use, but also difficult to counterfeit, the ECG-based technology is popularly used for continuous authentication to grant certain access privilege for users to identify a specific person. In addition, there are other

various applications that can be integrated with a continuously monitor for user's ECG and derive a quantitative measurement of their current stress state, fatigue, and disease, enabling users to understand their body's true state and take appropriate actions.

LITERATURE REVIWE

Riseul Ryu (2023) Biometric authentication systems may suffer from decreasing recognition performance due to varying environmental conditions and sample ageing, which cause intra-class variability. Adaptive biometric authentication systems have been proposed to address these deficiencies by dynamically changing their sampling and recognition processes in response to changes in the operating environment. This paper provides the complete discussion on the design of an adaptive biometric authentication system through a systematic review of the existing literature to date. The review shows that further investigation is required to target mobile and/or wearable devices as well as to consider a continuous authentication methodology. In addition to this, the evaluation of adaptive biometric authentications with large-scale datasets is required to validate the feasibility of the system and its scalability in real-world with a comprehensive study of evaluation metrics.

Abduraimov, O. (2022) The study is devoted to the study of the bio-morphological features of Elytrigia trichophora under conditions of introduction in the mountain semi-desert zone and the determination of their economic prospects for introduction into rainfed crops. The research results showed that, in the Tashkent area, the number of generative shoots is almost the same, but they are 30 - 31 cm long and the number of partial bushes is 4 - 5 more than in Chartak. The root system lengthens by 18 - 25 cm per year, and the number of roots of the first order in the third year of vegetation increases to 93.6 ± 2.31 pieces, they branch up to the III-IV order.

Rajendra Patil (2021) Over the last some years, a new era of engineering science has been recognized whose products are likely to create a huge bazaar in the immediate future. It has been known as "biometrics". The innovators of this fresh domain mean to construct strategies which would permit credentials of a person on the foundation of his/her "biological" features: vocal sound, diminuendos of movements, features of expression and other portions of the body, optic nerve or sword lily pattern. Nature has completed human presences with unlike appearances which may alter from one person to another. Biometrics talk about to the unconscious documents of a person built on his/her physiological or interactive characteristics. Through the distended addition of computers and Internet into our ordinary lives, it is essential to protect penetrating and personal data. Opposing biometric traits, PINs or PINs may be forgotten, and tokens like permits and driver's licenses may be forged, pinched, or missing.

Siddartha Thentu (2020) Robust authentication and identification methods become an indispensable urgent task to protect the integrity of the devices and the sensitive data. Passwords have provided access control and authentication, but have shown their inherent vulnerabilities. The speed and convenience factor are what makes biometrics the ideal authentication solution as they could have a low probability of circumvention. To overcome

the limitations of the traditional biometric systems, electrocardiogram (ECG) has received the most attention from the biometrics community due to the highly individualized nature of the ECG signals and the fact that they are ubiquitous and difficult to counterfeit. In this study, we contribute to creating a new large gallery off-the-person ECG datasets that can provide new opportunities for the ECG biometric research community. We explore the impact of filtering type, segmentation, feature extraction, and health status on ECG biometric by using the evaluation metrics.

Divya Nori (2020) Over the past year, approximately 10,000 Americans have died by psychostimulant overdose, and over 50% of these deaths were caused by prescription stimulant misuse. A comprehensive approach to detect a drug overdose in the environment where it occurs is imperative to reduce the number of prescription stimulant overdose-related deaths. Teenagers are at the highest risk for prescription stimulant overdose, so this study proposes a multi-factor overdose detection system named Hero which is designed to noninvasively operate within the context of a teen's life. Hero monitors five factors that indicate stimulant abuse: extreme mood swings, presence of amphetamine metabolite in sweat excreted from the fingertip, heart rate, blood pressure, and respiration rate. An algorithm to detect extreme mood swings in a teen's outgoing SMS messages was developed by collecting over 3.6 million tweets, creating groups of tweets for euphoria and melancholy using guidelines adapted from DSM-5 criteria, and training six Artificial Intelligence models.

Biometric and Authentication

A biometric is any measurable, robust, distinctive, physical characteristic or personal trait of an individual that can be used to identify, or verify the claimed identity of, that individual. Measurable means that the characteristic or trait can be easily presented to a sensor and converted into a quantifiable, digital format. This allows for the automated matching process to occur in a matter of seconds. The robustness of a biometric is a measure of the extent to which the physical characteristic or personal trait is subject to significant changes over time. Such changes may occur because of the effects of an individual's exposure to chemicals, aging, or injury. A highly robust biometric is not subject to large changes over time, while a low degree of robustness indicates a biometric that could change considerably over time. For example, iris patterns, which change very little over a lifetime, are more robust than voices. Distinctiveness is a measure of the variations or differences in the biometric pattern among the general population. The highest degree of distinctiveness implies a unique identifier, while a low degree of distinctiveness indicates a biometric pattern found frequently among the general population. The purpose of the biometric application determines the degree of robustness and distinctiveness required.

The biometric technology first process

This common approach is to gain access through the use of signs and assumptions that the owner of the sign and the proof identity will match. That kind model is called as single factor security. This technology is mostly used in house keyword system. This technology is also used for the identification purpose. This type of approach has a risk if the sign is

lost or stolen. Once any one enters with the key of another person, they could easily enter the house. This also happens with password. It will not be a secret someone else can use it. To overcome this problem goes for two factors security is find. This method is most cost and risks. The most common example of automated teller machine (ATM). With a card that shows who you are and PIN which is the mark you as the rightful owner of the card, you can access your bank account. The weakness of this security is that both signs should be at the requester of access. Thus, the card only or PIN only will not work Problems arise when you are forgetful person. Also, you often do not realize that the PIN is very personal thing. Basically, family or close friends may not know. The more sophisticated crime is to steal the PIN data from the source directly. In this situation, biometric fingerprint scanner can be a solution it is pretty exotic technology in the real world. It was basically used in police stations, high security buildings and even on PC keyboards purpose.

Types of Biometrics

There are basically two types of biometrics:

1. Behavioral biometrics
2. Physical biometrics

Behavioral biometric definition: Behavioral biometrics basically measures the characteristics which are acquired naturally over a time. It is generally used for verification.

Physical biometric definition: Physical biometrics measures the inherent physical characteristics on an individual. It can be used for either identification or verification.

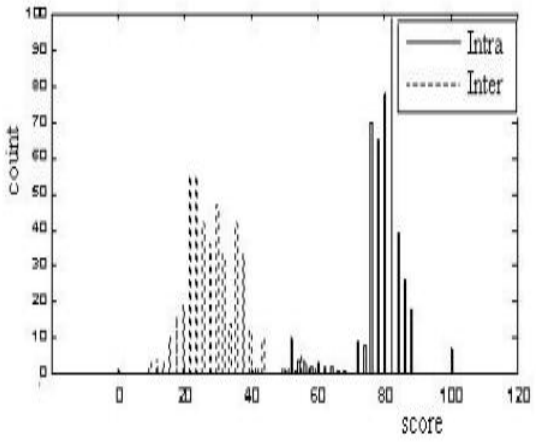
Design of Biometric recognition systems

Although humans have been using certain features (e.g. face, voice and gait) to recognize each other for thousands of years, the automated and semi-automated approach used in biometric recognition systems is a relatively recent development from the last few decades. While the mechanisms involved and the modalities (characteristics) used may vary, there are four basic stages in biometric systems: (i) enrolment, (ii) storage, (iii) acquisition and (iv) matching. With any biometric system, the individuals required to use the system need to be enrolled. Biometric data, for example a fingerprint, is collected using a sensor to produce a digital representation of the data. The system then extracts salient discriminatory features (i.e. feature extraction) from the digital representation and these features are used to generate a template (i.e. a feature data set), which is then linked to the user's identity and stored in the system. In basic terms the template takes the form of numeric data. The next time the individual presents his/her fingerprint to the sensor the sample template that is acquired is compared to the enrolled (stored) template using a mathematical algorithm. If they match the individual is accepted.

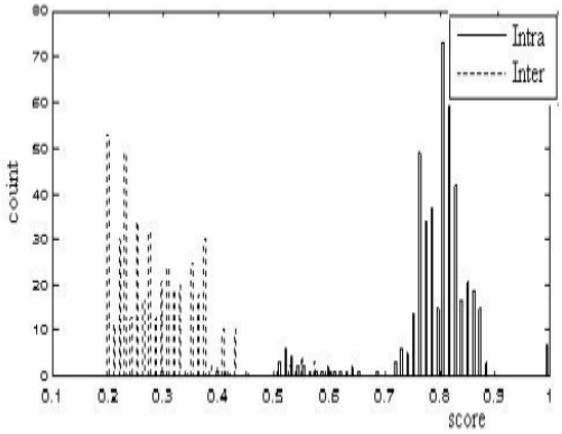
RESEARCH METHODOLOGY

To achieve this, a study was conducted by way of a systematic literature review following the steps addressed to identify the relevant research on adaptive biometric authentication systems. Retina, ear and palm print biometrics are used for verifying the authenticity of enrolled users in the proposed multimodal biometric system. The reason for choosing the above traits is that ear recognition is stable and non-invasive; retina recognition gives very high accuracy and palm print recognition has higher user acceptance. Images of ear, palm print and retina are obtained from the publicly available databases namely

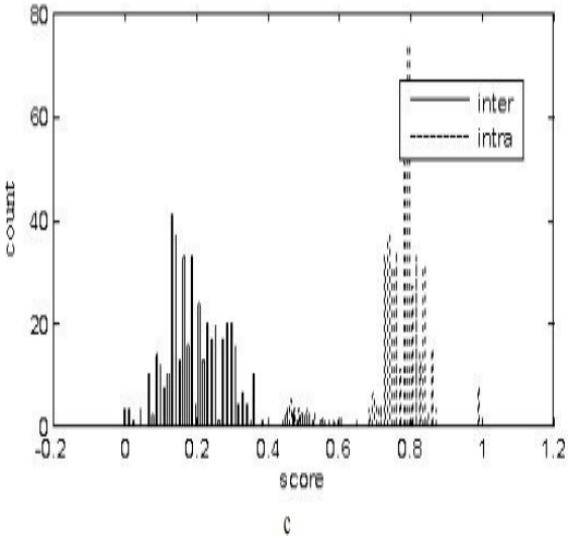
USTB, CASIA and VARIA respectively the generic view of the multimodal system based on retina, ear and palm print traits. Images of retina database are tested for similarity between users whereas ear and palm print images are tested for difference measure. As fusion requires matching scores of similar type, retinal scores are converted into equivalent distance scores as discussed which makes it possible to combine with the other two traits used in this system. It is also observed that distance scores of the above three traits occupy different range of values. Weights are assigned to the traits based on the individual recognition rates obtained during the authentication process. So min max normalization discussed is applied to convert the varying range of scores to a common range of (0-1). The key feature of any multimodal biometric system is the fusion of scores of various biometrics which enhances the performance of the system.



a



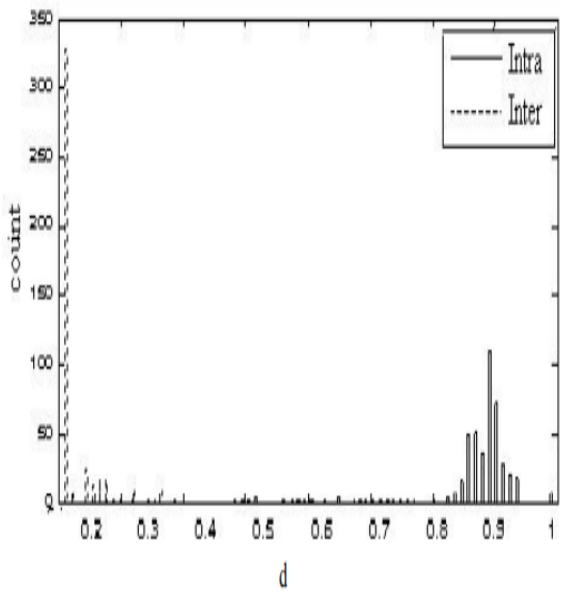
b



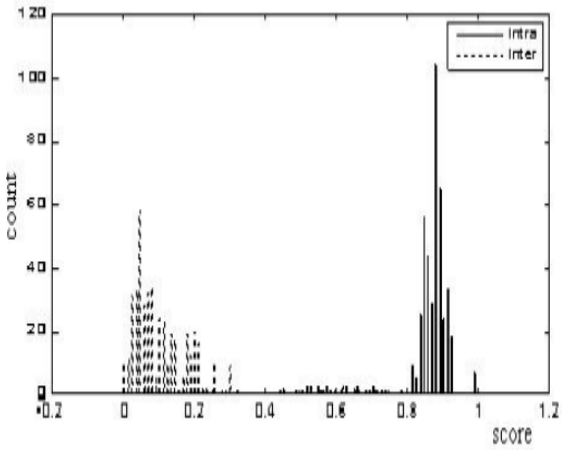
c

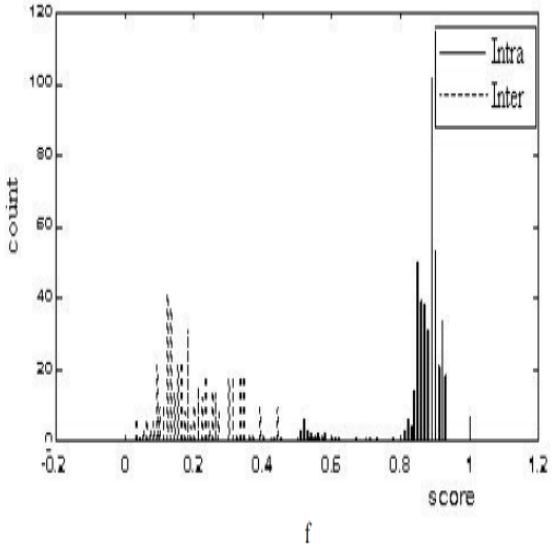
RESULTS AND DISCUSSIONS

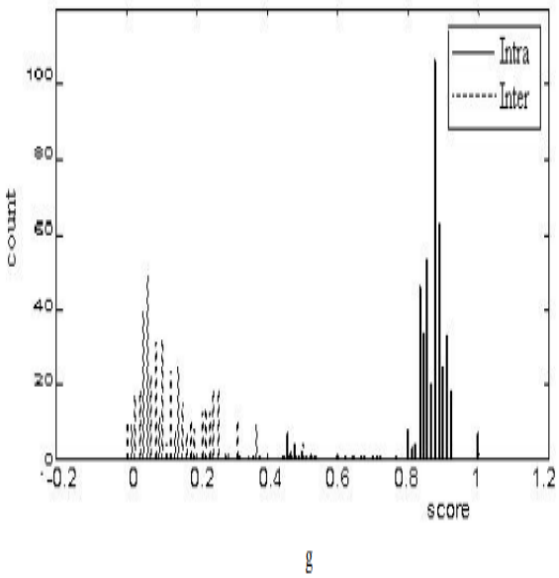
The matching score distribution of fingerprint is shown in Graph 1. It is found that MQQ method provides the largest separation between the two classes of scores compared to all other methods employed with fingerprint scores as shown in Graph 1d. Also QQ mapping performs equally well as seen from Graph 1e. It is observed that the remaining four methods show an average performance only.



Graph 1: Distribution graphs of fingerprint scores (contd.) (a) Raw scores (b) Modified min-max (c) Min-max (d) MQQ







Graph 1: Distribution graphs of fingerprint scores (contd.) (e) QQ (f) MQLQ (g) QLQ

CONCLUSION

This research work develops the basis for decisions on choice of efficient multimodal biometric authentication system needed for providing highly secured access to resources. The method involves blood vessel segmentation, feature template generation based on retinal minutiae (bifurcation points), which is insensitive to translational and rotational displacements of retinal images and finally matching of these points. Performance of the method was analyzed by using three publicly available retina databases. It was observed that there was a large inter-class distance for DRIVE images than STARE and VARIA images. As retinal template size and the effort involved in processing retina images are much less, this method is computationally efficient. This method involves two stages of feature extraction from the cropped portion of ear. The extracted feature points from each of the two stages of different ear images were then compared and the matching scores were computed. The final score was computed by combining the matching

scores obtained from the two stages by means of weighted sum fusion. It is also found that fusion of more traits increases recognition rate while decreasing the error rate, which ultimately raises the complexity of the biometric authentication system. Hence use of optimal number of traits is recommended which enhances performance of the system while keeping complexity within the limits. It is also observed that there is no specific method of normalization or fusion that can be quoted as the best one.

REFERENCE

1. *Rajendra Patil (2021), "Research Paper on Biometrics Security", Contemporary Research In India,ISSNno:2231-2137,*
2. *Israa Alsaadi (2015), "Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review", International Journal of Scientific & Technology Research,ISSNno:2277-8616,Vol.4(12),*
3. *Duncan S. Wong (2015), "Surveying the Development of Biometric User Authentication on Mobile Phones",IEEE Communications Surveys & Tutorials,ISSNno:1553-877X,Vol.17(3),Pages.1268-1293.DOI:10.1109/COMST.2014.2386915*
4. *Sayed, M. (2015), "Grobner Bases Method for Biometric Traits Identification and Encryption", Journal of Information Security,ISSNno:2153-1242,Vol. 6,Pages.241-249.*
5. *R. M. Chandrasekaran (2011), "Secured Electronic Voting Protocol Using Biometric Authentication",Advances in Internet of Things,ISSNno:2161-6825, Vol.1,No.2,Pages.38-50.*
6. *Hipos, A. (2018), "The Use of Biometric Attendance Recording System (BARS) and Its Impact on the Work Performance of Cabanatuan City Government Employees", Open Access Library Journal,ISSNno:2333-9721, Vol.5, Paages.1-10.*
7. *Divya Nori (2020), "Hero: Automated Detection System for Prescription Stimulant Overdose via AI-Based Emotion Inference, Metabolite Detection, and Biometric Measurement",Open Journal of Applied Sciences,ISSNno: 2165-3925,Vol.10,No.12,Pages.791-816.*
8. *Abduraimov, O. (2022), "Ontogenesis of Elytrigia trichophora (Link) Nevski in the Conditions of Uzbekistan (Biometric Indicators)",American Journal of Plant Sciences,ISSNno:2158-2750,Vol.13,Pages.1090-1099.*
9. *Riseul Ryu (2023), "The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction",ICT Express,ISSNno:2405-9595,Vol.9,Issue.6,Pages.1183-1197.https://doi.org/10.1016/j.icte.2023.04.003*
10. *Siddartha Thentu (2020), "ECG Biometric Authentication: A Comparative Analysis",IEEE Access,ISSNno:2169-3536,PP(99):1-1.DOI:10.1109/ACCESS.2020.3004464*