Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7, July 2021: 11345 – 11357

Research Article

User Identification and Validation for Interpretation - A Review

Ashwini K [1,a] and G N Keshava Murthy [2,b]

[1] Research Scholar, Department of Electronics and Instrumentation, Siddaganga Institute of Technology, Tumakuru , Karnataka, India.
[2] Assistant Professor, Department of Electronics and Instrumentation, Siddaganga Institute of Technology,
Tumakuru, Karnataka, India.

E-mail: [a] ashwini0429@gmail.com, [b] keshava.sit@gmail.com

Abstract:

The term security is more attractive in the present-day scenario in every aspect of life. This has encouraged the use of biometric authentication in almost all the fields where security is in need. Biometrics is associated with the human biological features which includes both the physiological as well as behavioral traits. The use of biometrics can be single modal or multi modal. Single mode uses only a particular human trait whereas multimodal includes a number of traits. However, use of multimodal techniques has shown a good success rate when compared to single mode. Use of biometric techniques provides a great advantage over already established techniques such as use of an ATM card, passwords, keys, pins etc…. where all these established techniques are harmful one or the other ways as the pins, passwords can be forgotten, keys and cards can be stolen. Thus the objective of using a biometric authentication system is to secure the most important information especially for the applications of military, naval and army.

There are a number of human traits that can be captured and a number of ways to capture these human traits. Finger print, ECG, EEG, voice, gait, key stroke dynamics, ear geometry, hand geometry, finger geometry, vein recognition are a very few techniques. This paper presents the introduction of such traits.

Keywords—authentication, single modal, multimodal, ECG, EEG.

INTRODUCTION

In the present scenario, countless things identify the uniqueness of a person like names, ID cards, bank account, Aadhar Cards, PAN cards, EPIC cards and so on. They are efficient means to represent the identity. However, all these identifiers can be counterfeited or copied with no trouble using a number of electronic gadgets. So, these identities cannot be trust worthy. Biometrics provide the most unique features that can be practically identified by devices and understood by computers so that they may be used as substitutions of our physical selves in digital world. This is how digital data can be bonded to the person's identity with long durability, reliable and unambiguity. It also helps in data retrieval in a rapid and automated manner. Biometrics involves the most unique features which include physical and behavioural characteristics of the individuals. Physical features such as finger print, face, palm print, ECG, EEG, EMG and behavioural

features include gait, key stroke, and writing style and so on. Biometrics means measure of life characteristics which will be unique, acceptable, universal and unambiguous.

Person identification using biometrics can be single modal or multimodal. Almost all biometric systems used in the current world applications are single modal and thus they depend on the evidence of a single source of information for authentication (e.g., single fingerprint or face). But these systems have to come across a variety of difficulties such as: (a) addition of noise in the acquired input like a scar in the fingerprint image, or an altered voice sample because of cold can be the cause of noisy data. Noisy data is involving faulty or improperly maintained sensors with which the data collected may include errors. As an example, there can be accumulation of dust on a fingerprint sensor or unfavorable ambient conditions like poor illumination of a user's face in a face recognition system may happen.
(b) Intra-class variations: this refers to interaction of users with sensors in an incorrect situation. This may also happen when the characteristics of a sensor are altered during authentication (e.g., optical versus solid-state fingerprint sensors).
(c) Inter-class similarities: while comparing the data of much number of users, due to overlap these errors may occur.
(d) Non-universality: sometimes when the system acquires the data, the required data may not be acquired which in turn is due to poor quality acquisition system. For example, a face recognition system may not capture the required features of the subject because of the movement of the subject.
(e) Spoof attacks: when behavioral characteristics like voice, gait, signature styles are used these types of attackers are most common. The voice of a person can be easily mimicked, the signature style of a person can be copied, the walking style can be easily mimicked. However, physical characteristics such as fingerprints, face are also susceptible to spoof attacks as, face of a person can be masked easily or finger prints can be easily copied. Thus, to overcome these limitations, multimodal biometric systems can be used to establish personal identity. The multimodal systems can be used to overcome most of the above identified problems of non-universality, spoof attack, inter and intra class variations and so on. Multi modal systems play a major role in eliminating spoof attacks since it would be difficult to spoof numerous biometric traits [20]. 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.

Biometrics can be planned under two phases: the enrolment phase and the identification phase. In the first stage called enrolment phase biometric traits are collected from an acquisition device which can be a fingerprint scanner, a iris scanner, an ECG device, an EEG acquition system or any other related devices. These sensed data is checked for its quality. If the quality is below threshold, the data will be acquired again. These data are later preprocessed if required and only the required data is collected and enrolling individuals and are accumulated in a database. On the other hand, in the second stage (i.e., identification phase), individuals present their biometric data for either identification or authentication purpose. The identification process is often referred to as a ‘one-to-many’ search) in the verification phase a ‘one-to-one’ match is done. Use of a successful matching algorithm renders a genuine authentication. However, use of single mode or unimodal biometrics is susceptible to many limitations such as spoofing, replay attacks, substitution attacks, tampering, masquerade attacks and Trojan horse attacks. Use of multimodal biometric system provides more advantage than unimodal systems as multimodal systems depend on two or more

individual data. It also improves recognition rate. Another advantage of multimodal biometrics is that different modalities might be more appropriate for different applications.

2.General Methodology Followed in Biometrics

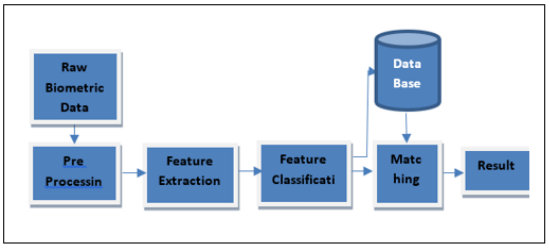

Figure 2.1: Methodology followed in biometrics

3.LITERATURE REVIEW

There are a numerous works carried out in the field of biometric technology using a number of biometric traits. A number of methods are proposed by authors using different algorithms for extraction and classification of features. The following are the few papers surveyed.

3.1 Tarfah Mohammed Alsultan et all proposed a method of biometric authentication, based on a comparative study using cloud computing. The author's view is to use biometric authentication in the sectors where very strong authentication is in need like IT resources. The author also has highlighted the pros and cons of using biometric data through cloud computing. According to the author, the use of cloud computing technology has a number of advantages however use of it in authentication needs complex protocols for specific applications using networks thus multimodal biometric technique is one of the best performing techniques for user authentication. They have uses three biometrics traits: two speech features and a face recognition system. The method of saving the traits in the cloud helps to secure the data and not only that the data's can be used whenever necessary by the use of internet. The author suggests the use of multimodal data acqusion not only to overcome spoof attacks, but also to use it in case where one of the data or the trait fails to be identified during matching. To overcome the complexities faced the author specifies to uses biometrics- as- a- service so that there occur several advantages like managing, limitability, availability, mobility and so on…multi modal systems has their own pros and cons. This system requires large amount of data availability, users may have bad experience, the system may become complex etc….. However, it has its own advantages like the authentication system can be secure, it may provide protection against spoofing, provides best performance, may be reliable etc….. [1].

3.2. Prasad K Saralaya et al focused and took a good initiative in using biometric authentication techniques for various online activities, especially in internet banking where people who do banking transaction online like NEFT, RTGS online instead of stepping out to the banks. But people need to keep their passwords in their memory which when forgotten or spoofed, user may lose their money. To overcome this, and to login without passwords, biometric traits can be used. In countries like India Aadhar is the main source of authentication now a days and these Aadhar contains authentication information like finger print, face and

iris. Thus, the user can use any of these to login. The author's view totally is to make the user experience better internet banking with complete feasibility [2].
The major problem arises when the system implements digital services. In case where people are digital illiterates and need to use the technology, they face a number of problems. The paper focuses on use of internet and computer enabled technology especially for senior citizens. The papers have used mixed method research which has given a fruitful result even for the aged population to adapt themselves for the modern technology. The authors in the paper have used finger print scanner technology to identify the user where this finger print scanned will be matched with the fingerprint of the user as in Aadhar. If the fingerprint is authenticated, the user will get an OTP as the second set of authentications. As the OTP is verified the user can complete his transaction accordingly. To make the system work effectively, the author has proposed several pre-processing steps to enhance the quality if finger print image scanned [2].

3.3. A paper based on Electroencephalogram especially for patients was proposed by Bhagya Shree et all. It was proposed mainly for patients, to reduce the false diagnosis of patients in hospitals. In the present scenario the number of patients approaching hospitals are raising day by day. Thus, mid identification of patients and mis diagnosis of them has been increasing. This may include wrong labeling of the patients or wrong administration of medication. To overcome this wrist bands, barcodes are currently in use. Though the rate of errors has been decreased using those, errors can occur in selecting a wrong wrist bands or wrong pass codes for them. To defeat such kinds of problems, use of biometrics can be a solution. This is because; biometrics cannot be stolen or forged. It represents unique behavioral or physiological identity of patients. Finger prints or face recognition can be used. However these systems have their own draw backs like, a dummy finger prints can be made, or the facial expressions of the persons may change. Thus use of the physiological traits like electroencephalogram, electrocardiogram can be used as they can be considered secured.

Electroencephalogram can be acquired using 8 channels, 32 channels, 64 channels and so on which is based on 4 brain signals, alpha, beta, delta, theta strating from 0 Hz to 14 Hz. Compared to other biometric triats, the individual EEG signal is based on individual metal arithmetic. The author has used cyton board, openBCI system, EEG lab along with matlab to complete the process. The results showed that even though the EEG signals were not accurate, the peaks and the shapes of particular persons are same and will not change [3].

3.4. The demand of security is a highly important task in case of using intelligent vehicles where thefts of such vehicles are becoming common now a days. To solve this issue, biometrics can be used. The author proposed new biometric trait using electroenchelogram where EEG can be used in the securing intelligent vehicles. The author has carried out a number of experimentations regarding this and has been successful in acquiring an accuracy of 87%.The author used 40 channel EEG amplifier and the experiments were conducted on young students. The author used 5 photographs of the subject where one photo was taken by the subject himself called target photo and remaining photos were randomly selected where each photo was displayed for 1000ms followed by 250ms of black screen. Totally the photos were display for 1250ms. Each picture uses the head part of the target.

Later the data was analyzed for both targets self and non-self-photographs. The results were decided based on the calculation of entropy, fisher distance etc.…according to the author, the system is sensitive for some reasons like selection of frequency, selection paradigm and subject condition [4].

3.5. Jaswinder Pal Singh et al surveyed on a number of biometric techniques based on gait recognition which depends on the walking pattern of the person. Person authentication is becoming a serious problem because of increased vulnerability. Such conditions have made us to use the video surveillance systems. Gait biometric techniques are one which is based on video surveillance. Because of its unobstructive and impalpable nature, gait biometrics has become one of the most common techniques in individual identification. The gait recognition system can be tracked even if the target is at some distance from the surveillance system and even low-resolution system can give good result without much cooperation of the subjects like in fingerprint, ECG, EEG, EOG etc... It is also very difficult to mimic the gait features of the targets. All these are added advantages of using gait as a biometric trait. Major applications where gait trait is uses can be in airports, railway stations, bus stations, metros etc.…. the gait recognition system used by the author is based on pattern classification where model based and model free patterns are used. The system was sensor based and vision based where sensor-based systems used where sensor-based systems used wearable and floor sensors and vision-based system uses marker based and marker free sensors. The sensor-based system used sensors which tracks the joint movements of the subject and the floor-based sensors was used to track gait patterns. After the collection of patterns, the gait feature extraction is done to reduce irrelevant or redundant data. The following were the LDA (linear discriminant method) for feature extraction. Genetic algorithm was used to solve optimization issues[5].

3.6.The author Shihab A. Shawkat et al proposed a method of biometric recognition based on hand geometry where the authors did not use any hardware. The system works on a specific algorithm based on neural network where the hand geometry was classified based on back propagation architecture. Experiments were carried out on 500 images of 50 persons and the accuracy of the result was 96%. According to the author, there are 30 widespread features in human hand and each feature differs from one person to the other. These features include finger length and width, palm width, position of palm and finger, distances between each finger, angle between fingers, hand thickness etc… the results of this frame work were satisfying. The calculation carried out were based on the hand movement, wrist diameter, palm's length, center finger thickness etc… the input will be taken using a camera where the photo of complete hand will be captured and processed. The method also identifies the person based on the texture and color of the hand. The process was carried out by taking a picture of the complete hand, converting them to gray image and later to binary. All the features were considered for classification such as finger lengths and width, palm area and the feature vectors were classified and saved in the data base. For classification the author uses neural network classifier and the accuracy obtained was 96.41% [6].

3.7. Kancharla, K et al proposed a handwriting signature recognition based on the strokes the user following while signing. Signature recognition is one of the behavioral biometric trait which is used for enormous number of applications. Signature biometrics can be taken in two forms, online and offline. Online forms is a dynamic form which considers the writing style of the subject. It counts the number of ups and downs, the stylus movement and its direction. Offline forms consider the signature as the image and compares these images with the template that is already stored. In the offline technique, the test image is compared with a number of templates already stored in the database. However, this needs lot of memory and time to save the templates. To overcome this the author has proposed a new method of offline signature identification using convolution neural network to gain high accuracy with minimal number of signature samples. A number of image processing techniques will be used to preprocess the signature samples which will reduced redundant data's such a background and noise. The author used 27 signature samples of different subjects and has got a good accuracy. The samples are converted in to gray image and further converted in to binary image. Later

a threshold is fixed and the values below the threshold will be considered as background. After applying the threshold, the image undergoes morphological processing where the result will be the background and the signature only. Later the image will be resized as all the images obtained may not be of a standard size which may become difficult to train using neural network. Further the evaluation is done by forming a number of layers and by calculating the precision values by considering the number of positive and negative classes [7].

3.8. The author Wang, Z et al proposed a new method of biometrics which uses ear as a trait since each one of us have different ear sizes and shapes. Apart from this ear geometry also provides most secure identification technique which will produce accurate result. The process includes edge detection, preprocessing, matching, inter level and intra level fusion. One more added advantage is that the ear geometry doesn't change after the age of 8 years and even if the facial expression changes. Along with this, ear biometrics can be captured using mobile phones and cameras and this can be done without the cooperation of the subject. However while capturing the trait, there can be a number of problems like addition of noise, pose, occlusion, poor illumination etc… but these problems can be overcome using different filters and through pre processing steps. A number of algorithms are used by the author like Adaboost, Morphological, fast R-CNN etc… The features of the ears are extracted based on different geometrical shapes. The author experimented on both unimodal and multimodal techniques and compared the results of both. Performance of Multimodal technique was good compared to unimodal technique [8].

3.9. Hesham Hashim Mohammed et al published a paper based on hand geometry for subject identification since fingerprint has its own disadvantage when used in large-scale and for the purpose of security. The author worked on 21 features of hand geometry. They worked on the data sets in 2 phases. The first phase includes data acquisition, pre-processing and geometric data collections such as length of each fingers, distance between the fingers, and width of each finger. The second phase includes testing and training using neural network algorithms. The 2^{nd} phase also includes feature extraction using 3 algorithms, the feed forward back propagation, neural network and Elman neural network. The result of using these algorithms is 95%, 92% and 88% respectively. The advantage of using hand geometry is that it needs small memory to store the data, it needs a camera or moderate resolution reader, user friendly and provides faster results [11].

The first step is acquisition of the hand image, converting it to gray image to eliminate background. Later the gray image is converted to binary image. A threshold is then selected and if the pixel value is above threshold output will be 1 else 0. The resultant image will have only the edges where these edges will be of only the high frequency components. To detect the edges, a canny filter is used and thus the features are extracted [11].

3.10. According to the author Juan Sebastian, mobile login methods using traditional ways, i.e., use of passwords, pins or figure prints are susceptible for attacks. This may help attackers or hackers to gain the information of the users. This use of biometrics techniques that can be collected from within the human body can be the best way to increase security. The authors have designed a platform in such a way that if the user touches two ECG leads, his ECG will be acquired and will be used for authentication. The algorithm used here detected the fiducial points LP, P, Q, R, S, T, and TP of the ECG. Once the fiducial points are detected, vectors are computed for each. Using this peaks and valleys will be found which will be different from person to person using hierarchical algorithm and stored in the data base. To detect the threshold, the author referred 4 databases available in physionet. And the threshold was selected based on batch process. The FAR was

just 1.30% and the TAR (total acceptance rate is around 84.93% during enrollment phase and the TAR is 96.16% and 1.49 % is the FAR for authentication phase [11].

3.11. The author M. Alva et all proposed a paper based on review techniques on Ear biometrics where ear biometrics can be one of the major reason for security as the human ears are all unique from one another. The shape of the ear does not change as the person grows by age. The author proposed three major steps wherein the first step involves preprocessing, the second phase involves feature extraction and the third stage involve authentication. Ear biometrics can be a good technique that can be used in person identification because of its unique features like ashelix, tragus, triangular fossa, concha, lobule, antihelix and crus helix. The added advantage is that the biometric features captured from the year does not change with change in facial expressions and it is unaffected by make up. These features mark as added advantage for the ear to be used in user authentication.

Steps involved in ear biometric authentication involves preprocessing, feature extraction, classification and decision making. While preprocessing is involved, feature based approach or intensity-based approach can be used. While feature extraction, geometric based approach or appearance-based approach can be used and while feature classification and decision making, SVM technique, Neural Network, K-Nearest Neighbor Technique or minimum distance classifier technique can be used [12].

3.12. The authors have proposed a biometric application using ear and have used in mobile applications for the purpose of security. In the applications of now a days developers use face or finger print recognisition. As a way which multiplies the security, multimodal traits can be used which may include ear biometric as the human ear has unique features and shapes. The author has used 2 set of databases which includes the 4 images of a person in 4 different angles. Colored images are used in the study as gray or binary images were not showing occlusions. The system works in 2 modes, one for collection of images to store in the database and the other to identify the user. In the first step, image is acquired, preprocessing is done, features are extracted and later this feature vector is classified and results will be viewed on the screen of the mobile device. As a preprocessing stage, image is down sampled, and converted into gray image and later histogram equalization is applied. The resulting image contains highlighted features and shapes of the ear. The haar-cascade transformation technique is used to identify the edge of the ear image. In the stage of feature extraction, LPB algorithm provides a good result where the difference in intensity values between the neighbor pixels is identified and the result is considered to be binary value. The descriptor is the histogram of these binary images. Later for the binary values which occur most frequently will be provided with unique code. The second algorithm used is the data reduction algorithm, principal component analysis which transformed the correlated data to uncorrelated data where the result of the first algorithm or second algorithm was used to store as the byte array in the database. In the third stage classification is done in using either Euclidean distance measurement technique or chi-square distance measurement. The algorithm compares the result of extracted array with already stored array in the data base. The result obtained was 90% for LPB algorithm and 100% for PCA algorithm. But when the camera was rotated to some extent, the results obtained were reduced yielding 65% for LPB and 55% for PCA [13].

3.13. A paper titled Biometric Security: Palm Vein Recognition Using Lbp and Sift was proposed by the authors Pooja et al where they implemented biometric authentication using palm vein vascular technology. The technique is unique as the arrangement of veins and arteries will reside in the subcutaneous layer below dermis and epidermis layer of the skin. This will be a added advantage as nobody can forge the individual information. The techniques of recognition is based on the flow of deoxidize blood within the veins. NIR

camera is used to acquire the image of the palm of the person where it produces dark prints for deoxidized blood flowing in the vein. These images will be captured, preprocessed and will be fed to the feature extraction algorithm. Later will be matched will saved data in the data base. The images acquisition can be touch based or contact free. The work has been done in such a way that it has no effect or minimal effect on transitional, scaling or rotational changes. The work has been divided in to 2 parts, the acquisition and training part and the rest is matching. The authors have used contact less palm vein acquisition system where the region of interest is first selected and then segmentation algorithm is applied to normalize the captured image. Later the normalized image is applied with some nonlinear functions so that the RGB patterns of the normalized image will be converted in to binary values and indexing for the threshold will be done. Later a low pass Gaussian filter is applied on the image where it reduces darkness and blends the disc size. The method is based on identification junction points, the distance between index finger and middle finger and and the distance between middle finger and ring finger. These junction points are arranged in ascending or descending order and the slope and angle of inclination is found out. Next, to enhance the contrast of the image, contrast enhancement technique followed by histogram equalization to normalize the image. This helps in showing the vein pattern clearly. To get the exact vein pattern, LPB or SIFT algorithm is used. For matching current template is matched with stored templates. The performance of the system using PPB algorithm is very good compared to SIFT algorithm [14].

3.14. The author Felix Marattukalam et al proposed a new method of contactless palm vein biometric recognition method. The method uses the vascular patterns of the palm beneath as it is more accurate and unique compared to the veins at the backside of the palm. Use of palm vein trait provides an accurate result as it has more features for human authentication. The system provides good FAR and FRR. As an initial step the person whose identity to be authenticated has to hold his palm in front of a contactless palm scanner for few seconds. The image aquation system consists of a IR sensor which illuminates the structure of the palm along with the finger guides in an appropriate ways. Later the system consists of USB interface, software development kit and required drivers. The IR sensor records the image at a wavelength of 760nm. This wavelength will be absorbed by the deoxygenated blood flowing in the veins and the arteries reflect it back. The camera records the dark network of veins as the as an image. This image is used further for comparison and matching. The capture images will be of low contrast, so the ROI of the image is selected based on the segmentation of multi spectral palm images. Further, the image quality is enhanced using methods such as filtering, denoising, histogram processing, contrast stretching etc…. the features are further extracted using Affine Invariant Transform and Ridge let Transform. Feature extraction is an important step in palm vein recognisition as it is the final step in comparison and authentication. The authors concluded by comparing the performance of different palm vein recognisition system [15].

3.15. Mohit Ingale et al proposed a comparative analysis of Biometrics using ECG. The major intension of the authors was to use a large data base which includes ECG of numerous persons to help people working on biometrics. The authors explored the impact of different filters used, classification techniques, segmentation and matching. The authors have proposed a new filtering technique used before the classification of ECG and they have also provided a complete assessment result for the assorted ECG databases. To illustrate the efficiency of the proposed work the authors have worked on around 1119 subjects. The work showed 100% accuracy, 1.2%, 1.48% and 0% EER, FAR and FRR respectively. The recording was done both on-the-person and off-the-person. On-the-person recording was made directly from the body of the person by using electrodes and electrode jelly. A number of leads to record ECG was used. In on-the-person recoding the capture methods and can be directly controlled. But it may cause some

discomforts to the patient. However, the ‘‘off-the-person’’ recording utilizes devices to measure ECG signals and does not require any special preparation of the subject with objects or surfaces. Once the ECG data is been acquired, the first step is to preprocess where the data will be isolated from high frequency and low frequency noise. To remove them, extended Kalman filter is used which provides state vector and observation vector respectively. Later IIR filter is applied to obtain the transfer function which results in the coefficients of the numerator and denominator. The next step is to segment the ECG signal in to 5 peaks, the P, Q, R, S and T. the main goal of segmentation is to find the repetition of ECG signals and thus helps in reduction of template size which smoothness template matching. In the proposed work the peak wave, the R signal is identified and the distance between the peaks before R and after R are detected which is called fixed length segmentation. This covers the majority of ECG signal. In the next step feature extraction is done by following the fiducial or non-fiducial points. Fiducial points depend on P, Q, R, S and T waves which depends on the heartbeats based on temporal or altitudinal difference between different peaks.

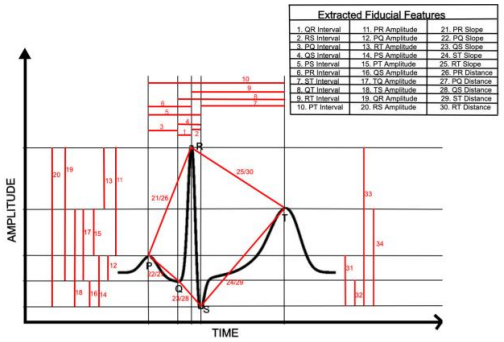

Figure: 2.1: Typical ECG showing fiducial features

These temporal and altitudinal features differ from one person to another. However, the fiducial feature extraction is difficult in case of abnormal ECG’s. Thus use of non-fiducial points are most commonly used. When non fiducial features are used, frequency analysis or time analysis algorithms are applied to obtain statistical features. The authors have used Symmlet and Daubechies algorithms to obtain statistical features. Later to compare the acquired ECG with ECG in database Euclidean distance and Dynamic Time Wrapping is used. When Euclidean distance measurement techniques is used, the feature vectors of both acquired and database ECG signals are matched and if it matches, the person will be authenticated, else, the person will be rejected. The DTW algorithm finds the ideal alignment between two ECG sequences with different lengths, such that the sum of the differences between each pair of aligned points is minimal. This method helps to compare the ECG in the database with the acquired ECG. If they are not aligned the length changes and thus matching done not happen and the person’s identification will be rejected.

3.16. The authors Ho J. Kim and Joon S. Lim proposed a biometric system by considering ECG as the variable. They have worked on 73 subjects taken from physionet were experimented by using neural network with weighted fuzzy membership function. Normalization and ensembling is made during the stage of preprocessing, features are extracted using Haar-transform and training or classification is done using neural network. The ECG signals were first sampled and normalized during the preprocessing phase, later Haar transform was applied to train the preprocessed data sets. Later the classified signals were saved in the database. Once a new data set is received, the matching is done based on the saved data. ECG samples are normalized for the reason that the sampling rates of the data differs from one instrument to another and also the intensity of heart beat also will differ bases on whether the subject is on medication. Thus, the processes of normalization is very important. Further the in the ECG signal, the P-wave and the T-wave may vary with

respect to time on the time axes but the QRS complex in unchanged. In order to obtain stable features, ensembling is done. The features are then extracted using Haar wavelet transform which is to process the ensembled signals in to various frequency bands. The classification is done based on high and low frequency bands. Later neural network function is used to categorize the weighted inputs from the trained values. The neural network with weighted function consists of three layers, the outer layer, hyper box layer and outer layer. The input node has many layers. The node in the hyper box is multiplication of number of nodes in input and output layer. To authenticate the subjects using ECG data, each biometric ECG signal will be connected to one input nodes which are authenticated and unauthenticated class nodes of outer layer. The author gradually increased the number of ECG data and calculated the true acceptance rate and false acceptance rate which were 98.20% and 5.84% respectively for 1 heartbeat [17].

3.17. The author Hui-Ling Chan et al elaborated on the advantages and disadvantages of using EEG as biometrics. The advantages of using EEG as a biometric trait is that it is unique from each human, it is universal, distinct and it is superior when compared with other biometric techniques. However, it has its own disadvantages like even though the performance of the system is good, acquisition of signal realistically may be difficult. The subjects participated in the real world are only once or few times. But using it in biometrics, the subject should participate frequently which sometimes need an operator to acquire the signal. At the same time the system should identify the person even if he provides his biometry after a span of time. Constant changes in the brain wave over time or with respect to the emotions of the person must also be identified. If the number of subjects increases in the data base, the system may find it difficult to authenticate users. So, to over come these difficulties the authors have provided few suggestions which includes use of multimodal data, to have user friendly design, to ensure completeness of implementation, to model physiological changes, use two stage system to minimize false acceptance rate and to increase true acceptance rate [19].

4. Pros and Cons

Trait	Pros	Cons
Face	Person identification is easy even in a massive crowd	Identification is difficult in case of low-resolution camera
	Identifies through facial features.	May provide false result in case capturing is done under bad lighting condition.
Iris	Requires high resolution camera to capture.	Very hard to adjust scanning device.
	Provides highly accurate result.	Iris scanner is very costly.

Finger Print	Speed of verification takes very less time	Takes time to register finger print in data base
	It is a best secure technique.	Difficult to capture ridges when there is a cut or burns.
EEG	Highly accurate technique for person identification.	Capturing EEG signals is bit difficult as electrode on the scalp are to be used.
	Highly recommended for its universality and uniqueness	Classification of alpha, beta, delta, theta and gamma signals may take time.
ECG	Very accurate as it cannot be spoofed.	May not get accurate result in case where person suffers from abnormalities.
Voice	Need not to train and classify the data set.	Difficult to use for the person with speaking disability.
	Helpful for people who are handicapped.	Voice can be mimicked.

5. Conclusion

This paper has provided a brief introduction of different biometric authencation techniques which included face, ear, signature, key stroke, ECG, EEG, palm vein etc. The results obtained while using multimodal techniques were accurate compared to single mode biometric as multi modalities of a single subject will be under consideration. If one of the person identification fails, the remaining may succeed. Meanwhile these biometric techniques can be used in numerous applications where security is majorly considered.

References:

[1] Tarfah Mohammed Alsultan , Asiya Abdus Salam , Khalid Adnan Alissa, Nazar Abbas Saqib, "A Comparative Study of Biometric Authentication in Cloud Computing", 2019 International symposium on networks, computer and communication(ISNCC).

[2] Prasad K Saralaya, Anjali R and Dr. Subbareddy K V, "biometric authentication usage for internet banking" 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017, India.

[3]. Hy Do; Vu Truong; Kiran George; Bhagyashree Shirke, "EEG-Based Biometrics Utilizing Image Recognition for Patient Identification", 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 10.1109/UEMCON47517.2019.8992962.

[4]. Yuhua Chen, Jinghai Yin, "Design of electroencephalogram authentication access control to smart car", Healthcare Technology Letters, 2020, Vol. 7, Iss. 4, pp. 109–113, doi: 10.1049/htl.2019.0092.

[5]. Jasvinder Pal Singh, Sanjeev Jain, Sakshi Arora, Uday Pratap Singh, "A Survey of Behavioral Biometric Gait Recognition: Current Success and Future Perspectives", Archives of Computational Methods in Engineering, Springer publications, 2019.

[6] Shihab A. Shawkat , Khalid Saeed Lateef Al-badri , Ahmed Ibrahim Turki, "The new hand geometry system and automatic identification", Periodicals of Engineering and Natural Sciences, Vol. 7, No. 3, September 2019, pp.996-1008, ISSN 2303-4521.

[7]. Kancharla, K., Kamble, V., & Kapoor, M, "Handwritten Signature Recognition: A Convolution Neural Network Approach", 2018 International Conference on Advanced Computation and Telecommunication (ICACAT), doi:10.1109/icacat.2018.8933575.

[8] Mohit Ingale , Renato Cordeiro , Siddartha Thentu, Younghee Park, And Nima Karimian , "ECG Biometric Authentication: A Comparative Analysis", IEEE Access, volume 8, 2020, Digital Object Identifier 10.1109/ACCESS.2020.3004464.

[9]. Wang, Z., Yang, J., & Zhu, Y. (2019). "Review of Ear Biometrics". Archives of Computational Methods in Engineering. doi:10.1007/s11831-019-09376-2 . Springer publications.

[10]. Hesham Hashim Mohammed, Shatha A. Baker, Dr. Ahmed S. Nori, "Biometric identity Authentication System Using Hand Geometry Measurements", Journal of Physics: Conference Series, ICMAICT 2020, doi:10.1088/1742-6596/1804/1/012144.

[11]. Juan Sebastian, Arteaga-Falconi, Hussein Al Osman and Abdulmotaleb El Saddid, "ECG Authentication for Mobile Devices, IEEE Transsactions on Instrumentation and Measurement, volume 65, No. 3, March 2016.

[12]. Michelle Alva, AnuradhaSrinivasaraghavan, Kavita Sonawane, "A Review on Techniques for Ear Biometrics", 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 10.1109/ICECCT.2019.8869450.

[13]. Milos Oravac, Jarmila Pavlovicova, "Mobile ear recognition app", IWSSIP-2016, 23rd international conference on systems, signals and image processing 23-25 May, Bratislava, Slovakia.

[14]. Pooja, Vinay Bhatia, "Biometric Security: Palm Vein Recognition Using Lbp and Sift", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-11, September 2019, DOI: 10.35940/ijitee.J9370.0981119.

[15]. Felix Marattukalam and Waleed H. Abdulla, "On Palm Vein as a Contactless Identification Technology", 2019 Australian & New Zealand Control Conference (ANZCC), Auckland, New Zealand. November 27-29, 2019.

[16] Mohit Ingale, Renato Cordeiro , Siddartha Thentu , Younghee Park, and Nima Karimian , "ECG Biometric Authentication: A Comparative Analysis", DOI: IEEE ACCESS.2020.3004464, VOLUME 8, 2020.
[17]. Ho J. Kim and Joon S. Lim, "Study on a Biometric Authentication Model based on ECG using a Fuzzy Neural Network", 4th International Conference on Advanced Engineering and Technology (4th ICAET), IOP Conf. Series: Materials Science and Engineering 317 (2018) 012030 doi:10.1088/1757-899X/317/1/012030.
[18]. Sandra Persiani, Bilge Kobas, Sebastian Clark Koth, Thomas Auer, "Biometric Data as Real-Time Measure of Physiological Reactions to Environmental Stimuli in the Built Environment", Energies 2021, 14, 232, DOI:10.3390/en14010232.
[19] Hui-Ling Chan , Po-Chih Kuo, Chia-Yi Cheng, Yong-Sheng Chen "Challenges and Furutre Perspectives on Electroencephalogram- based Biometrics in person recognition", Front. Neuroinform., 09 October 2018 https://doi.org/10.3389/fninf.2018.00066.
[20] Waleed Dahea , HS Fadewar, "Multimodal biometric system: A review", International Journal of Research in Advanced Engineering and Technology, Volume 4; Issue 1; January 2018; Page No. 25-31.