COMPARATIVE STUDY OF COMPUTATIONAL INTELLIGENCE PARADIGMS FOR INTELLIGENT ACCESS CONTROL BASED ON BIOMETRICS METHODOLOGIES

Shaymaa Adnan Abdulrahman¹, Mohamed Roushdy², Abdel-Badeeh M. Salem³

¹Department of computer Engineering, Imam Ja'afar Al-Sadiq University
Baghdad, Iraq

²Faculty of Computers & Information Technology, Future University in Egypt,
New Cairo, Egypt

³Department of Computer & Information Science, Ain Shams University,
Cairo, Egypt

¹shaymaaa416@gmail.com

Abstract

Intelligent access control is one of the challenging tasks in the human identification, image analysis, and diagnoses disease and computer vision. The focus towards the intelligent access control has been increased in the last years due to its various applications in different domains. For this reason, it was used intelligent access control to facilitate the task of identifying the human. The objective of this paper is to analyse and evaluate the seven techniques for the intelligent access control and advantage and disadvantage of each type. In addition, represents biometrics characteristics in general. The Biometric feature is used to determine human identity including the brain signals. Through this study, brain signals are the best among the techniques. In this study, we first presented a survey of the Computational intelligence techniques in biometrics. All previous studies used brain EEG signals. Where different algorithms were used to extract, the features. These feature applied for human identification. The Accuracy achieved was up to 97% according to the studies found in this research.

Keywords: Computational intelligence, human identification, Biometrics, Fingerprint, EEG signals.

I. Introduction

The human identification system can be having any types of the human trait such as face, iris, fingerprint, palm, lips, etc. (Dhillon and Kalra, 2017). For this reason, intelligent access control has become necessary and important in our time.
The access regulated by use a set of rules that specifies who is allowed getting access what is the constraint on such access. At this time, need more advanced technique to control access through fast advances in innovation over the previous year’s (Connor and Ross, 2018). In spite of Biometric refers to the evaluate and analyzes of the feature of a living creature. Biometric applications are contain having number of perspectives which are applied for the analytics of various features from human outlook or even inner segment. Usually in biometric attributes cannot be lost, transferred, stolen, high, security. Due to fact that these attribute is very difficult to reshaping again and it requires areal user to log in.

Accordingly to the conditions that are used as a basis for a good biometric are: (Wang, 2016). **Universality**: This implies that an individual need to possess features. It is not realistic to obtain 100% encasement because there are many people without fingers, mute people or people who have injured eyes. These situations should be catering for. **Uniqueness**: Which implies that two different individuals should not have the same biometric characteristics? **Permanence**: This implies that there should be no variation in characteristics and with time. **Collectability**: which implies that the measurement of features should be done in a quantitative way and taking out the features, which should be simple. **Performance**: This means the achievable identification/verification, resources, accuracy environmental or working states needed to obtain an acceptable accuracy. **Acceptability**: This shows the extent people are ready to embrace biometric system. **Circumvention**: This explains the difficulty faced in fooling the system through fraudulent techniques.

Usually biometric detection is one of the most important stages in recognition systems and can be classified into five principle categories such as (Nanni, et al., 2015): **Collect data**: by scrolling a website and eliciting data. **Arrange the input data**: at the exact time of having this data, there is a necessity to insure about its format if it is useable or not. **Analyze the input data**: the analyze data by using mathematical expression, or statistical, or algorithms. **Train and testing**: in this steps training and testing the algorithm. **Evaluating**: in this step, analyzing the result generated by the proposed approach.

With regard about choosing in such research. It is necessary to search technique that gives us high performance and accuracy .These technique is used for identification or authentication person. The aims of this study are comprehensive survey of these techniques that used for intelligent access control based on Biometrics. Analyzing large amounts of techniques to predict which one is better for intelligent access control according to security execution time, memory capacity. In addition, the advantages and disadvantages of each techniques and results obtained by the suggestions of researchers and dataset used in these techniques.

The paper is structured as follows: Section 2 : Related Works Section 3: Biometrics verification schemes such as (Fingerprint ,Face ,Hand geometry ,Iris, Keystroke ,Signature ,Voice, EEG ) Section 4: Results and Discussion Section 5 : Conclusion .

---


*Shaymaa Adnan Abdulrahman et al*
II. Related Works

In this section we will search several types of the Computational intelligence techniques used in biometrics. Specially using EEG signal as a biometric feature.

According to (Carmen, et al, 2015) has proposed the utilization of brain wave (EEG) in identifying individuals. Most of the EEG-based biometrics systems choose facts fiducially features from the EEG wave property. Was proposed the utilization of non-fiducially features through the Hadamard Transform (HT) with eighteen subjects undergone at Boston's Beth Israel Hospital as dataset. There was no bias in the subjects that can enhance the identification task. Pass-band filter with a range of 0.67 and 45 Hz was used in the second stage. The accuracy was up to 97% when used a K-NN as classifier. (Ma Lan, et al, 2015) was proposed the utilization of convolutional neural networks (CNN) to analyze the performance of individual's best. EEG data was obtained from Resting State with Closed Eyes (REC) and Resting State with Open Eyes (REG). Ten subjects were analyzed for 55 seconds individually for both REC and REO. The obtained results showed that CNN-based joint-optimized EEG-based Biometric System was 88% as classification.

(Zhendong Mu, 2015) stated that Rough set theory has been successfully employed in different information mining fields. Because a lot of researchers are using EEG to examine the biological signals in electrical brain research. The EEG feature extraction algorithm has become a main study content. EEG acquisition is the use of a 40-Neuroscan amplifier. Pass-band filter was between 200Hz-0.05Hz when applied thirty subjects. Each subject used 200 EEG with a total of 6000 EEG. Subject identifies the proportion of 70% or more of accuracy. (Wael Khalifa, et al, 2014) was applied artificial immune system inspired approach for identifying users when used EEG signals. The Physionet EEG Motor/Movement/ Imagery dataset is used to validate approach [VI]. The dataset comprises of signals of over a hundred users. The dataset is imported to EEG lab for the pre-processing phase. Then artificial immune system based algorithms for user matching was used. (Urmila, et al, 2018) was proposed EEG signals emitted from a live functions brain are establish to individual to every human. The raw EEG signal passes through FIR Band pass filter so that the unwanted signal is removed. Multi scale Wavelet Packet Decomposition and Multi scale Shape Description are used for feature extraction from the EEG signal. The sub-bands correspond to delta, theta, alpha, beta and gamma frequency bands of the brain signals. From the five segments. Three are utilized to train Error Correcting Output Code Support Vector Machine classifier. While the other two sections are utilized to test on the educated model. (Koike, et al, 2016) brain waves obtained through person-grade EEG equipment to explore its capabilities for human identification and authentication. The dataset was obtained from the statistical significance of the P300 component in event-related potential (ERP). This experiment was applied to fourteen channels with twenty five subject. The result appeared over 96.7% utilizing just a solitary 800 ms ERP age. Also, (Emanuele, et al, 2018) was utilized the investigation of the longitudinal conduct of EEG signals. Markov models used as classifiers when forty - five subjects were applied in the experiment. The accuracy was good up to 80%.
Distinguishing people from electroencephalogram (EEG) signals dependent on eye flickering waveforms was proposed by (M. Abo-Zahhad, et al, 2015). Database of 10 subjects is gathered by utilizing Neurosky Mind wave headset. Two calculations are actualized for auto-backward displaying in particular called Levinson-Durbin and Burg algorithm. Linear and quadratic discriminant functions are tested. System can identify subjects with best accuracy of 99.8%.

(Feng Lin, et al, 2018) represented another psychophysiological convention by means of non-volitional mind reaction for reliable portable confirmation, with an application model of keen headwear. Especially address the accompanying exploration challenges in portable biometrics with a hypothetical and observational consolidated way: How to produce dependable cerebrum reactions with advanced visual upgrades. How to obtain the unmistakable mind reaction and examine extraordinary highlights in the versatile stage. How to reset and change cerebrum biometrics when the current biometric accreditation is disclosed. Accomplished a f - score exactness of 95.46%.

III. Biometrics Verification Process

Biometric is can be explained as a quantifiable physiological and/or behavioral attribute that can be encapsulated and analogize to an occurrence at the lime of verification (Feng Lin, et al, 2018). Biometric technology is defined as any method that reliably utilizes tangible physiological or behavioral characteristics for distinguishing one individual from another. The origin of biometric technology is traceable to about several thousands of years back. Biometric system can be performed using two different types of modes. Including authentication and enrollment. In the latter, the individual's biometric features have been changed by the biometric system into a digital form and then store the result in another storage system (Nawasalkar, 2013). Figure 1 describes the registration process for the biometric system.

Fig. 1: Registration process for biometrics systems

However, the biometric system is designed to be used for an identification or confirmation process in authentication mode. During the confirmation procedure, the biometric system verifies the identity of the user by making a comparison between the recorded features with the template; this process has been illustrated in Figure 2.
The security domain can be used in various approaches of authentication; these approaches are familiar such as a password, PIN, or piece of private information; smart cards and card keys, or token such as a Secure ID card; and/or a biometric (Ain, et al., 2016). Biometric characteristics are often categorized based on behavioral or physiological nature. The latter is connected to the shape and the color of the body. The patterns include retina and its recognition, fingerprint, hand geometry, hand palm veins, DNA chains, face recognition, and palm print. However, behavioral characteristics are connected to the person’s behavioral patterns which include voice, gait and rhythm of typing (Manisha and Sudeep, 2016).

In biometrics. A few parts of this description have required a preparation. All biometric identifiers have been examined to be partitioned into two major gatherings (Agarwal, et al., 2017). Physiological and behavior as illustrates in figure 3. Biometric confirmation frame-works are not 100% precise. There are two types of flounders in a common bio-metric frame-work. A bogus reject (FR) error is the termination of a confirmed individual endeavoring to get the framework. A false acknowledges (FA) blunder is the acceptance of an individual who does not know exactly who the person is. These two types of errors are conversely correlating and when all is said in done can be strained by the edge of certainty. The boundary can be extended to extend the security of the frame-work, which has been decreased FA blunders and builds FR errors (Alessandra and Loris, 2017).

![Biometrics verification process](image)

**Fig. 2:** Biometrics verification process

![Biometrics classification](image)

**Fig. 3:** biometrics classification
III.i. Physiological Biometrics:

III.i.1. Finger Print

Fingerprints have been the best quality level for individual ID inside the legal network for multiple hundred years. Fingerprints and fingerprints combine to give the most dominant methods for individual distinct evidence accessible to police and courts. The basic examples of finger-prints are circles, loops and curves that can be set up in finger-prints (Sharma, et al., 2015). So finger print acknowledgment is broadly used due to its reliability. Finger print is broadly utilized in legal and business applications, for example, criminal examination, internet business also, novel ID cards as shown in figure 4 (Kaushal and Kaushal, 2011).

![Figure 4: Finger print Definition](image1)

Fingerprints consist of some usually, confronted accordingly named designs. There are mainly more five examples such as arch, tented arch, right loop, left loop and whorl (Christophe, 2017). Finger knuckle print can be very helpful for individual character. Finger knuckle as another biometric approach which providing immense extension for specialists in few of years. Out about this finger impression will be extra standard biometric method and need been utilized to particular ID number more than 100 a longtime. That unquestionable quality might be because of those methodologies that fingerprints never show signs for change Also no two fingerprints would be identical (Waghode and Manjare, 2017). The Finger print scanner is public security boundary which can be found in a wide range of top of the line gadgets that are as of now available everywhere. Its quick and simple to utilize, it is utilized as an option or a supplement for the difficult recalled passwords, it has been also utilized by the requirement of law to discover the doubtful; yet it has been utilized to recognize the good person also, shown Figure 5 (Tripathi and Goyal, 2017).

![Figure 5: Finger print scanner](image2)
III.i.2. Face Recognition

Amid the entire history of mankind, individuals utilized face to recognize individuals from each other (Alsaadi, 2015). Facial acknowledgment is a PC tool that naturally recognizes or confirms an individual accompanied by the assistance of an advanced picture or video out-line from a source of the video. One of the strategies to do the concerned procedure is to contrast the specified precedent and the precedents in the database as shown figure 6 (Xu, et al., 2018).

Fig. 6: Example of face scanning

Face recognition can be considered as a standout amidst the most fruitful biometric discernible verification methods included in a few kinds of biometric distinguishing proof. Face admission has been used as a validation operation in different domains and especially in PC security associated exercises, for example the security of country, criminal ID, building access, a client distinguishable verification in cell phones and etc. Face acknowledgment likewise assumes a noteworthy job in the exploration field of biometric and PC vision. The objective of a face acknowledgment framework is to have an immaterial misclassification. The face recognition is a PC framework that distinguishes the static picture or on the other hand the face picture in powerful video, matches with the put away face database in PC, and afterward performs single or numerous faces distinguishing proof (Mantoro, 2018). Face acknowledgment innovation is a sort of physiological component acknowledgment in the field of acknowledgment. Many features lead to the variance of a single face images that contribute to the recognition problem complication, if they cannot be prevented by careful pattern of the capture state. Inadequate limitation or handling of such variance definitely leads to recognition failures (Guo and Zhang, 2018). These consist the following:

- **Physical Variations**: expression of face changing, growing up, appearance of person such as (facial hair, makeup, hairstyle, glasses, camouflage).
- **Obsession Geometry Variations**: the change in scale, position and in-plane turning of the face (facing the camera) and the turning of the depth (presentation of a profile that faces the camera indirectly or not the full front face).
- **Imaging Variations**: lighting change; camera types; channel properties (for broadcast or compressed images).
• **Imaging changes**: lighting change; camera types; channel properties (especially for broadcast or compressed photos).

### III.i.2.1. Face Recognition Technology

In this section, some of the technologies has been briefly reviewed which have been utilized for face recognition. Generally, face recognition frame-works proceed to distinguish the face in an image with the effect of interpretation and normalization for interpretation, scaling and in planning rotation (Mostafa, et al., 2018). When a normalized image is output, the global or local features are extracted and compressed with a compact face display that can be stored in a database or a smart card and make a comparison with face displays obtained later. In natural, it must be in the image before recognizing a face. In some cooperative systems, the face detection function is eliminated by making customer detection. Generally, systems use a combination of skin tone and facial tissue to locate a face and use an image pyramid to allow the detection of faces of different sizes. Progressively, systems have been developed to detect faces that are not fully front (Mostafa, et al., 2018).

There is a remarkable diversity in the way the face appearance is decoded for confirmation by a programmed frame. Currently, different diverse frame-works underway and the most appropriate one can be based on the field of application. A remarkable disparity in the methodologies is whether the appearance or geometry of the face is to be mentioned (Klemen, et al., 2017). Geometry is difficult to measure with any precision, especially from a still image alone, but it provides greater stability against masks and aging. Appearance data are obtained immediately from a face picture, but are progressively submit to shallow diversity, especially from position send feedback.

Face recognition is firmly identified with numerous different areas, and offers a rich basic writing with huge numbers of them. For distinguishing of countenances in video, the face following is vital, imagination in a very three measurements with the head evaluation presents (Bapat and Kanhangad, 2017). This normally prompts evaluation of the individual's focal point of consideration. This normally prompts estimation of the individual's focal point of consideration and evaluation of look, which are critical in person PC communication for understanding the purpose.

### III.i.3. Hand Geometry

Hand geometry can be described as the utilization of geo-metric state of a hand for acknowledgment goals. This strategy was somewhat well known for 10 years’ prior however these days it is only from time to time utilized. The strategy depends on the style that the situation of the hand of one individual varies from the situation of the hand of someone else and does not alter afterward a specific age (Kumar, et al., 2003). Be that as it may, but it is not distinct, shown figure 7.
While hand geo-metric characteristic is broadly utilized to execute biometric recognition, greater part of the strategies utilizes pictures gained against a uniform foundation. In the event that division of the hand is executed, existing systems can be utilized in jumbled foundations too. In hand geometry you can Two prime methodologies have been researched for segmenting hand from non-uniform surroundings for hand geometry constructed approaches, skin identification and background deduction (Mostafa, et al., 2019). Skin-based partitioning is very powerful for a uniform background, but fails in the existence of skin-colored items in the background. Background sub-traction methods, generally, are unaffected by the background. However, they affected even from tiny back-ground changes which cannot be sidestepped. A small amount of storage space is required to save the hand geometry model as con-trasted to the palm-print (Angadi and Hatture, 2018). While the condition of the skin (i.e., dirt, dirt, scars, etc.) did not affect the quantifications of hand geometry, the palm-print required a proper sigh of base lines, wrinkles and tissue to remove the feature vector. Handheld images can be selected with cheaper devices, i.e. camera, but the palm-print images require larger and more expensive scanners. Based on the data which has been used for personal verification, human hand reading technologies can be divided into three classifications (Angadi, and Hatture, 2016):

- Palm technology,
- Hand vein technology,
- Hand geometry and hand shape technology

The first category can be considered the classical process in the hand biometrics. The methods, which have been utilized here, are similar to those utilized for fingerprinting. The size, the shape and the flow of papillae are assessed and the details are the prime features in the verification process. Image preprocessing and standardization in this approach gives us binary image involving papillae and their span. When shooting images, the palm consists of five areas due to different lightning. Although it certainly speaks medically, considering muscles, it has only three regions (Puneet and Phalguni, 2018). The palms are the lower palms, the middle palms, the upper palms, the palms (thumb portion) and the hypotenary (small finger part). The position of these regions has been shown in Figure 8.

Fig. 7: Example of hand scanning

Shaymaa Adnan Abdulrahman et al
Second category can be utilized in a very similar approach for taking the hand image, however as opposed to utilizing conventional scanner and/or camera it rather utilizes specific gadgets involving the scanners with an infrared light or any other innovation which can be utilized for recovering picture of duct beneath the human skin (Abdulkareem, et al., 2019). Hand-vein biometrics is picking up prominence at the most recent years, and almost certainly, this will be one of the fundamental biometric attributes for what's to come. Utilizing contactless methodology for catching the construction of human veins allows promising outcomes in this field.

Third category can be defined as a hand geometry and hand-shape each human hand is one of a kind (Geetika, 2013). During 2002, thirty comprehensive features of the geo-metric of hand were defined. These characteristics are very precise, but can be represented as comprehensive features of contactless 2D hand geometry. The creators have characterized as shown in the Figure 9

**Fig. 8: Palm areas**

II.4. Iris Recognition

The iris can be defined as a fluffy rounded diaphragm which locates between the lens and cornea and of the human eye. The iris is cribiform near to its core by a rounded hole which is known as the pupil. The capacity of the iris is to observe the measure of light which has been entered through the pupil, and this is finished by the sphincter muscle and the dilator muscles which adapt the area of the pupil (Khalaf, et al., 2019) as in figure 10. They are even distinct for the congruous twins. Iris can be applied for different authenticity and security execution that involve ID cards and passports, prison protection, data-base access and computer log-in, boundary control and government schedule. Iris biometric is more dependable and precise when it compared to other bio-metric features such as finger-print. Iris tissue is firm all over
The iris scanner does not require any specific lighting circumstances or any specific light type (dissimilar to the infrared light which required for the scanning of retina). There are two techniques for using the eyes features for authenticity. First one can be based on the recognition of retina (Kien, et al., 2019). The person has to gaze in a device that operates a laser based scanning of his/her retina. The specific device anatomized the vessels of blood arrangement of the desired retinal image. Incidentally, it validates the person. This arrangement of blood vessels is distinct for each eye. The device is not genial because the user has to confirm a point when laser is analyzing the eye (Harakannanavar and Puranikmath, 2017). It looks alike hard to cheat on the authentication system. The second method is iris based recognition. The scanner has to work by using a camera. Dissimilar to the retinal procedure, the user does not need to be near the device to be verified. The provided picture is analyzed by using the device, and it contains 266 various spots. It is known that it is the most authentic biometric verification method. Moreover, iris is still the same through the entire life.

III.ii. Behavioural Biometrics

III.ii.a. Key Stroke

Keystroke Dynamics can be referred to one of the common and cheap behavioral Biometric applications, which utilized in recognizing the user authentication when the user is writing by using the keyboard. In the PC security field, the simplicity of information access by the reliable user is a large domain of investigation (Lichao, et al., 2017). Keystroke Dynamics method has been developed. A distinct technology for authenticity by means of key-stroke dynamics by removing various features of the user’s beats during typing a text on the keyboard is utilized in this technique. The detailed schedule when every key has pressed and when it has released during the typing on computer keyboard are including: dynamics of key-stroke, key-stroke bio-metrics, typing dynamics and recently typing bio-metrics. Keystroke dynamics formula has been used for permission and authenticity by examining the typing performance of its users such as beating pattern, over-all speed, and common errors (Mohammed, and Al-Khateeb, 2016) as shown figure 11.
Shaymaa Adnan Abdulrahman et al.

III.ii.b. Signature

The signature which has been done by handwriting checks and ID has been roughly partitioned into two classifications: online and offline (Bay, et al., 2017). Figure 12 show these techniques differs in sort of data they utilize, in offline technique, the signature which has to be confirmed is saved as an image and processed as pixel models or textures, in online technique the signature can be captured by a special pen which works electronically through production in addition to static attribute is also captures the dynamic features such as pen location, physical force, angle, elapsed time to sign in, and etc. (Abdulrahman, et al., 2019; Hafemann, et al., 2017).

The dynamic signature is a biometric quality broadly utilized and acknowledged for checking an individual's personality, Current automatic signature-based biometric approach regularly require five, ten, or significantly more examples of an individual's user to learn intrapersonal fluctuation adequate to give a precise check of the person's personality (Leghari, et al., 2017). On-line signature verification systems are depending on two techniques feature- or time functions-based systems (global and local systems). Signature is a biometric property made by a mind boggling process starting in the underwriter's mind as an engine control "program", executed through the neuromuscular system and left on the composition surface by a handwriting device. The mainly aim of signature based biometric authentication with forensic application is the protection of crime.

III.ii.c. Voice Recognition

Human voice conveys extraordinary character for everybody. It has been seen that there is critical change between each individual’s discourse signals. Thusly, discourse flag is likewise as remarkable as human unique mark. To construct a client recognizable proof framework, biometrics speaker recognition system is inescapable.

Fig. 11: Keystroke dynamics

Fig. 12: Signature biometrics
(Muttaqi and Mousavinezhad, 2018). See figure 13. Biometrics speaker recognition procedure consequently perceives the discourse of an individual dependent on the feature exists in his/her voice signal. The human voice is the most regular method for correspondence between Human creatures, so extraction unmistakable characteristics of biometric voice varieties can be an effective answer for creating appropriate encryption keys rather than trouble keeping arbitrary keys created in memory and far from unlawful clients like PIN or secret key (David, et al., 2016). Voice distinguishing or verification technique are very significant to multi-facets of the world today, like identifying a person’s ID over phone for other services of security such as the connected Internet of Things (Boles and Rad, 2017).

![Voice recognition](image)

**Fig. 13:** Voice recognition

### III.ii.d. EEG Signals

Electroencephalogram (EEG) is an observing technique for cerebrum movement that records it electro-physiologically, shown figure 14 (Hui-Yen, et al, 2017). EEG signal is recorded from a subject by setting electrodes on the scalp. EEG estimates voltage changes of the cerebrum. These changes are made by the ionic current inside the neurons. Biometric application on electroencephalography (EEG) distinguishes people by utilizing individual qualities in human brainwaves (Abdulrahman, et al., 2020) (Rajendra and Yuki, 2019). Biometric Based on EEG system have been generated by different studies. Some studies utilized the data-set of BCI contest using multiple traits, involving AR co-efficient, linear complication, energy spectral intensity, and phase synchronicity (Pozo-Banos, et al., 2014). Brain Computer Interface (BCI) technique, which supplies an electronic interface directly and can transport commands and messages instantly from the human brain to a computer.

EEG is one of the most active capturing techniques that can be utilized in bio-metrics because of its hardware devices evolution. It is a very unique, secure and cannot be replicated method. Besides that, EEG signals are biodynamic and possess a proof of aliveness for a particular individual. Thus, it cannot be duplicated like most of the other static physical biometric techniques (Abd Ghani, et al., 2020). For security sector, three kinds of authentication are used, including your information, such as your password, PIN code, or piece of personal information (such as your pet’s name); your possession such as your smart card, or token; and/or a biometric (Mohammed, et al., 2017). The obsession protocol is usually classified into three various classes. Through these signals, various work such as the applications of medical field like (brain dis-order, motion sick-ness, smoking, alcoholism, detection and diagnosis,
sleep disorder, brain tend. In addition, the execution of an EEG based biometric system relies on the main design of the protocol.

Fig. 14: EEG Signal

IV. Results and Discussion

In this study, portray the latest CI based techniques in the previous studies for each progression of the biometric identification. Specifically, we present the most pertinent issues and the primary procedures used to adapt to them, with a particular spotlight on the most basic biometric characteristics, for example, the iris, fingerprint, and face. The procurement of the biometric test is the initial phase in the acknowledgment procedure, and is performed with the guide of biometric devices (e.g., optical scanners for fingerprints, advanced cameras for the face). Therefore, Computational Intelligence can be utilized for a more powerful and versatile procurement, by playing out a self-alignment of the sensors, or a programmed discovery of blunders in the tuning procedure. The quality of biometric tests greatly affects the presentation of biometric frameworks. Quality measurements are then utilized to foresee the acknowledgment execution of an example, with the goal that higher quality esteems compare to a superior acknowledgment of the people. Nevertheless, assessing the correspondence between an example and its acknowledgment capacity can be unpredictable. Thus, CI procedures have been regularly utilized right now become familiar with the connection between an example and its quality. The nature of biometric tests significantly influences the introduction of biometric structures. Quality estimations are then used to predict the affirmation execution of a model, with the objective that higher quality regards contrast with a prevalent affirmation of the individuals. In any case, evaluating the correspondence between a model and its affirmation limit can be erratic. Along these lines, CI systems have been consistently used right currently become acquainted with the association between a model and its quality. The quality to the uniqueness of the example, and in to evaluate the quality dependent on all encompassing face attributes.

CI methods have been applied for the improvement of biometric tests, particularly on account of fingerprint images. Actually, varieties in the position and applied weight of the finger on the sensor can cause locales of the picture where the subtleties of the fingerprint, explicitly the edges and valleys, are not unmistakably characterized.

Shaymaa Adnan Abdulrahman et al

575
Hence, a preprocessing task is utilized to level out the nature of the picture before removing the attributes.

This section presents the result and explanation of our analysis in this study. Some techniques are distinct from other. In this study, we first presented a survey of the Computational intelligence techniques in biometrics. All previous studies used brain EEG signals. Where different algorithms were used to extract, the features. These feature applied for human identification. Accuracy was up to 97% according to the studies found in this research, shown as Table 1.

**Comparative analysis for previously used Techniques Table1:**

<table>
<thead>
<tr>
<th>NO</th>
<th>Authors</th>
<th>Extraction Feature</th>
<th>Subject</th>
<th>Classifier</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Carmen Camara et al</td>
<td>Hadamard Transform (HT)</td>
<td>18</td>
<td>KNN</td>
<td>0.97%</td>
</tr>
<tr>
<td>2</td>
<td>Lan Ma, et al</td>
<td>Convolution Neural Network (CNN)</td>
<td>10</td>
<td>-</td>
<td>88%</td>
</tr>
<tr>
<td>3</td>
<td>Zhendong , Mu</td>
<td>Rough Set</td>
<td>30</td>
<td>-</td>
<td>70%</td>
</tr>
<tr>
<td>4</td>
<td>Wael H. kalifa, et al</td>
<td>Rough Set</td>
<td>100</td>
<td>Artificial immune system</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Koike, et al [19]</td>
<td>Pass-band filter</td>
<td>25</td>
<td></td>
<td>96.7%</td>
</tr>
<tr>
<td>6</td>
<td>Emanuele Maiorana ,</td>
<td>Pass-band filter</td>
<td>45</td>
<td>Markov models</td>
<td>80%</td>
</tr>
<tr>
<td>7</td>
<td>M.Abo-Zahhad et al</td>
<td>Levinson-Durbin and Burg algorithms</td>
<td>10</td>
<td></td>
<td>99.8%</td>
</tr>
<tr>
<td>8</td>
<td>Feng Lin, et al</td>
<td>Statistical feature</td>
<td>-</td>
<td>SVM</td>
<td>95.46%</td>
</tr>
</tbody>
</table>

Biometric frameworks are as a rule progressively utilized for the identification of people in security uses. The structure of such frameworks, nonetheless, requires handling diverse mechanical regions at the same time by managing all perspectives in a coordinated manner. In this study, CI assumes a key job, since it gives the chance to structure versatile and evolvable frameworks, tolerant to fragmented and uncertain information. This study has investigated recent advances in Computational intelligence paradigms for intelligent access control based on Biometrics Methodologies, CI strategies that spread all the means of biometric identification. The proposed study indicated that CI strategies are empowering advancements for expanding the exactness and power to non-idealities with regard to customary algorithmic methodologies, and that distinctive CI approaches can be effectively used to play out all the undertakings of the biometric acknowledgment process.
Specifically, we imagine that ongoing strategies like profound learning and Convolutional Neural Networks will be progressively concentrated soon so as to additionally expand the presentation of current biometric frameworks.

Table 2: Advantages and disadvantages of biometric

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Biometrics presents evident points of interest over secret phrase and security based on token</td>
<td>- Execution is falling apart by oil, dust, water on the finger surface.</td>
</tr>
<tr>
<td>- The best application of biometric innovations is the programmed fingerprint recognition for volatiles security from an examination of the systems’ necessities: security, roughness, estimation, the factor of usability structure, protection and functional temperature extend It is developing and very much demonstrated center.</td>
<td>- It Can't be utilized in synthetic industrial and medical clinics since utilization of synthetic compounds can change the unique mark design in hands.</td>
</tr>
<tr>
<td>- This innovation has a high exactness</td>
<td>- It Is highly connected to forensic.</td>
</tr>
<tr>
<td>- It is the most researched and standardized technology of biometric</td>
<td>- It causes a loss in protection and security.</td>
</tr>
<tr>
<td>- It desires more accumulation for the format of biometric</td>
<td>- The problem of forgery by artificial, spoofed, gummy or fake fingers.</td>
</tr>
<tr>
<td>- It is exceedingly steady, and unchangeable with age - which is the opposite of facial and voice acknowledgment</td>
<td>- Bigger data-base required for the recognition of fingerprint and signature. Picture Capturing division feature normalization extraction comparison result</td>
</tr>
<tr>
<td>- It is a cheap equipment with low power consumption</td>
<td></td>
</tr>
<tr>
<td>- It has a high responsibility, implies it can monitor client's movement like who, what and when.</td>
<td></td>
</tr>
<tr>
<td>- It gives advantageous and extra security to the framework.</td>
<td></td>
</tr>
</tbody>
</table>

Through our studies and analyzes of biometrics, we found that there are some advantage and disadvantage in it. Table 2 illustrates this. Then we chose seven techniques such as finger print, Face, Iris, Keystroke, Signature, Voice, EEG. These techniques differ among themselves according to quality, cost, performance, accuracy, easy to use ...etc. Table 3 contains The advantages and disadvantages for each type of biometric By the characteristics of each techniques, It found that using brain signals (EEG) as biometrics Has a good performance and accuracy was 97% according to Carmen Camara et al. Especially when obtained information or data from person's head by using sensors like electrodes. These electrodes are available and easy to use. In addition these electrodes consist of feature like if one electrode breaks down, it can be, removed immediately and every electrode montage, can be realized easily. All of these characteristics make EEG technique the best in
identifying a person or diseases diagnosis, in addition high performance and accuracy as we mentioned earlier.

Table 3: Advantages and disadvantages of each type of biometrics

<table>
<thead>
<tr>
<th>Biometric</th>
<th>Advantages</th>
<th>Disadvantages</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>fingerprint</td>
<td>1- very secure method</td>
<td>1- Portable fingerprint can be considered as a very easy to steal method</td>
<td>Israa M. Alsaadi</td>
</tr>
<tr>
<td></td>
<td>2- they have been used to lock or unlock gadgets and applications without waiting to remember passwords</td>
<td>2- inexpensive components in the structure can cause an authorized person to be denied by accessing due to a little sweat on the finger or an improperly cut</td>
<td>Ludwig Lester F</td>
</tr>
<tr>
<td></td>
<td>3- very simple method, cheap and faster to set-up</td>
<td>3- Damage, whether short or permanent, can interfere with the control operation</td>
<td>Duvenaud</td>
</tr>
<tr>
<td></td>
<td>4- It is also a stand-out among the most generated bio-metrics</td>
<td>4- it is feasible to create copies with the fingerprint to imitate the person</td>
<td>David K and Maclaurin Dougal</td>
</tr>
<tr>
<td></td>
<td>5- mall storage size desired for the bio-metric format that lessens the extension of the data-base desired memory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Face</td>
<td>1- No connect required</td>
<td>1- May be influenced by hats, glasses, hair.</td>
<td>Teddy Mantoro, et al</td>
</tr>
<tr>
<td></td>
<td>2- Available sensors</td>
<td>2- Face change during age</td>
<td>Xiaoxiang Xu, et al</td>
</tr>
<tr>
<td></td>
<td>3- Easy to use</td>
<td>3- Influenced by lighting or expression</td>
<td></td>
</tr>
<tr>
<td>Iris</td>
<td>1- Stable over life time</td>
<td>1- May be fooled by pictures</td>
<td>Essam-Eldean, et al</td>
</tr>
<tr>
<td></td>
<td>2- More dependable and precise when it compared to other biometric features such as fingerprint</td>
<td>2- When acquisition iris image, it requires more training than most Biometrics</td>
<td>Geetika, and Manavjeet Kaur</td>
</tr>
<tr>
<td></td>
<td>3- No connect required</td>
<td>3- Complicated when to capture for some individuals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4- very high secured</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keystroke</td>
<td>Signature</td>
<td>Voice</td>
<td>EEG</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------</td>
<td>-----</td>
</tr>
<tr>
<td>1- No additional hardware</td>
<td>1- classifications, online and offline</td>
<td>1- No connect required</td>
<td>1- Stable over time</td>
</tr>
<tr>
<td>2- Continuous monitoring</td>
<td>2- Captured by a special pen</td>
<td>2- Used sensors like telephones, microphones</td>
<td>2- subject must be alive</td>
</tr>
<tr>
<td>3- Minimum training</td>
<td></td>
<td>3- Permits user to run a computer by speaking up</td>
<td>3- available sensors like electrodes</td>
</tr>
<tr>
<td>4- Neither registration nor authentication affect the steady work-flow because the user would require tapping text anyhow</td>
<td></td>
<td>4- Permits command of text</td>
<td>4- Difficult to Forgery and Theft</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5- Removes-handwriting and spelling troubles</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6- Always spells in a correct way which doesn't often recognizes words correctly.</td>
<td></td>
</tr>
<tr>
<td>1- May be High false reject rate</td>
<td>1- Narrow range of applications</td>
<td>1- Not sufficiently distinctive for Identification and verification over large data-base</td>
<td>1- Lengthy registration process.</td>
</tr>
<tr>
<td>2- High Sensitive to change in keyboard</td>
<td>2- Difficult to control sensor</td>
<td>2- Easy by pass by recorders</td>
<td>2- High processing</td>
</tr>
<tr>
<td>3- Range of applications is narrow</td>
<td></td>
<td>3- need large storage to store voice folder</td>
<td></td>
</tr>
<tr>
<td>4- Key-stroke dynamics are non-static bio-metrics the same as voice</td>
<td></td>
<td>4- Hard to utilize in class-room settings according to noise disruption</td>
<td></td>
</tr>
<tr>
<td>5- Low precise. Key-stroke dynamics is one less uniqueness bio-metrics.</td>
<td></td>
<td>5- Getting errors which can be complicated without sufficient support</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6- Aids with one level of the writing procedure but it is not a solution for the writing problems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Rybnik Mariusz, et al
Sun Lichao, et al
Hafemann Luiz G, et al
Tolosana Ruben, et al
Andrew Boles, and Paul Rad
Acharya U Rajendra, et al
Chungho Lee, et al

Shaymaa Adnan Abdulrahman et al
V. Conclusion

Intelligent access control is one of the challenging important like human identification, image analysis, and diagnoses disease and computer vision. The focus towards the intelligent access control has been increased in the last years due to its various, applications in different domains. For this reason it was used intelligent access control to facilitate the task of identifying the human. The study contains comparative analysis for previously used Technique. Summarized advantages and disadvantages of biometrics systems. Comparison each of techniques according to performance and accuracy as indicated. Through our study, it found that used EEG signals, as biometrics is the best technique compare to with seven other techniques. Finally there are still many aspects of intelligent access control. Some type’s techniques can be used as Multimodal biometric systems to increase accuracy and performance. Multimodal biometric systems combine multiple sources of biometric, features. As well as some feature extraction has been superficially, explored but require future study, to be completely understood.

References


VIII. Angadi, Shanmukappa and Hatture, Sanjeevakumar "Hand geometry based user identification using minimal edge connected hand image graph", IET Computer Vision, vol 12, no 5, pp 744-752, 2018.


XIII. Connor, Patrick and Ross, Arun "Biometric recognition by gait: A survey of modalities and features, Computer Vision and Image Understanding”, vol 167, pp 1-27, 2018


XXI. Gupta Puneet, Gupta Phalguni "Multibiometric authentication system using slap fingerprints, palm dorsal vein, and hand geometry", vol 65, no 12, pp 9777-9784, 2018


XXX. Madane Manisha, Thepade Sudeep, "Score level fusion based bimodal biometric identification using thepade's sorted n-ary block truncation coding with varied proportions of iris and palmprint traits", Procedia Computer Science vol 79, pp 466-473, 2016


Shaymaa Adnan Abdulrahman et al
LIII. Xiaoxiang Xu, Li Zhang, Fanzhang Li MSSVT "Multi-scale feature extraction for single face recognition", 24th International Conference on Pattern Recognition (ICPR), August 2018 20-24.


LVI. Zhendong Mu: EEG Feature Extraction Based on Rough Set, 3rd International Conference on Management, Education, Information and Control (MEICI), 2015.