International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET2310012

An Empirical Investigation of Human Identity Verification Methods

Bhavesh Kumar Jaisawal*[1], Dr. Yusuf Perwej[2], Sanjay Kumar Singh[3], Susheel Kumar[4], Jai Pratap Dixit[5], Niraj Kumar Singh[6]

[1*]Scholar (B.Tech Final Year) Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, India

[2]Professor, Department of Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, India

[3]Assistant Professor, Department of Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, India

[4]Assistant Professor, Department of Computer Science & Engineering, Ambalika Institute of Management & Technology, Lucknow, India

[5]HoD (IT), Associate Professor, Ambalika Institute of Management & Technology, Lucknow, India

[6]Assistant Professor, Department of Information Technology, Ambalika Institute of Management & Technology, Lucknow, India

Article Info

Publication Issue :
Volume 10, Issue 1
January-February-2023
Page Number : 16-38

Article History
Accepted : 01 Jan 2023
Published: 15 Jan 2023

ABSTRACT

A recognition technique is essential in practically every industry in the current digital era. It has several advantages and may be used for security, identification, and authentication. The relevance of access control systems based on biometrics has grown in recent years since they have the ability to address the majority of the shortcomings of existing security systems. Automated biometric systems for human identification take a measurement of the body's "signature," compare it to a database, and make an application-specific determination. These biometric methods for personal verification and identification are based on physiological or behavioral traits that are usually recognizable, despite changing over time, such as fingerprints, hand geometry, the face, voice, lip movement, gait, and iris patterns. The purpose of this study is to conduct a thorough literature review in order to pinpoint the most well-known recognition techniques, applications, and obstacles.

Keywords : Biometrics System, Recognition Techniques, Biometric Databases, Face Recognition, Fingerprint, Hand Gesture, Gait Recognition.

I. INTRODUCTION

The prevalence of phoney identities is one of the major issues that individuals in today's society face. Recognition technologies are becoming more and more common as we transition to the digital world [1]. The method of confirming an individual based on behavioral and physiological traits is known as biometric authentication. In recent years, approaches based on biological characteristics of humans have become increasingly important in identifying persons, whereas pass codes, OTP [2] generation, and other security measures have the potential to be lost, misapplied, or faked, among other things. Therefore, biological traits that are difficult for anybody to access, such as facial identification [3], fingerprints, palm prints, iris, retina, and signatures, can be utilized. Verification and identification are the two main goals of facial recognition. Applications for face recognition are important in the following areas, including criminal case investigation, general identity verification, camera surveillance, database management systems, smart card-based applications, and security investigation [5].

Methods for face recognition are often available. Currently, one of the most talked-about subjects in computer-related research is facial recognition [6]. The majority of these studies concentrate on the algorithm's performance with a certain set of samples. However, several studies also pay attention to how the adoption of facial recognition would affect society on a social level. Face recognition begins with the detection of face patterns in sometimes cluttered scenes, moves on to normalizing the face images [7] to account for geometrical and illumination changes, and may use knowledge of the position and appearance of facial landmarks. Finally, the results are post processed using model-based schemes and logistic feedback [4]. The iris is a highly significant component of the human body and one of the physiological biometrics because of its stability and uniqueness. Iris recognition technology is now more advantageous in the [8] fields of information security and person authentication in the areas such as regulating access to security zones, verifying travellers at airports and stations, controlling computer access at defense establishments, research companies, controlling data base access in distributed systems, etc. Many nations presently employ the iris recognition [9] system to identify people with national id cards, flight crews, and airport workers.

In recent years, automatic hand gesture recognition has grown in importance. The adoption of several non-contact based apps and devices has expanded as a result of an increase in the number of deaf and hearing impaired people [10]. Modern technology has advanced, and it now plays a significant part in systems for human-computer interaction. The primary form of communication for the deaf, the hard of hearing, and the non-verbal is sign language [11]. However, these groups have obstacles when interacting with others who do not comprehend sign language on a regular basis [12]. The term "biometric" refers to a science that examines a person's physiological or behavioral characteristics for security purposes. The phrase is derived from the Greek terms "bios" (which means "life") and "metrikos," which means "measure." The biometric traits are difficult to fabricate, imitate, guess, or steal. These biometric procedures don't need memory. Biometric identification methods are used to distinguish between individuals based on their physical traits. Physiological biometrics employs fingerprint, face, palm print, iris, retina, ear, DNA [14] etc. to recognize individuals, whereas behavioral biometrics uses voice [13], keystroke, stride, etc.

II. Related Work

These days, technology seeks to convey enormous knowledge-based technological advancements [15]. This face detection technique in [16] really determines whether or not the image is a facial image. The actual detection procedure utilises the Haar Cascade classifier. Paul Viola and Michael Jones [17] suggested an efficient approach for object recognition called object detection utilising Haar feature-based classifiers. A technique based on machine learning uses photos to train a cascade function. It is employed to find items in other pictures. Using SIFT and SURF characteristics, Bakhshi et al [18] technique classifies facial pictures, and the PCA method is used for improved matching outcomes when faces are rotated or their emotions alter. The results demonstrate that the suggested technique performs better than previous methods in terms of recognition rate. Different illumination invariant approaches were looked at by Poon et al. (19), who chose the one that works well with PCA for face recognition. According to experimental findings, implementing the Gradient Faces approach at the pre-processing stage can significantly increase the recognition rates. By contrasting the Receiver Operating Characteristics (ROC) curve, the authors of [20] conducted research to find the optimal facial recognition algorithm (Eigenface and Fisherface) offered by the Open CV 2.4.8 and then integrated it in the attendance system. The ROC curve demonstrated that Eigen face outperforms Fisher face based on the studies conducted in this research. A system that used the Eigen face algorithm has a 70% to 90% accuracy rate. By integrating Discrete Wavelet Transforms (DWT) [22] and Discrete Cosine Transform (DCT) [23], authors in [21] suggested a way for a student attendance system in a classroom utilising facial recognition approach. Following the use of Radial Basis Function (RBF) [24] for categorising the facial objects, these algorithms were employed to extract the characteristics of the student's face. The accuracy rate for this method was 82%.

A novel iris segmentation approach based on the Daugman's integro differential operator IDO was proposed by Radman et al. [25]. This method consists of three main modules: removing reflections; iris and pupil identification using a quick IDO; and live-wire eyelid detection. The iris picture is complemented to eliminate reflections, the holes a collection of dark pixels surrounded by lighter pixels and inaccessible from the edge of the image are filled in, and the resulting image [23] is complemented once again. In order to complete the segmentation, the IDO looks for parameters of the circular iris and pupil borders over the whole picture. A complicated parabolic model is then employed by the IDO to localise eyelid boundaries. The author compared this segmentation algorithm's recognition performance to that of cutting-edge iris segmentation techniques. Training and testing are the primary two processes in design, according to E. Elfakhrany and Ben Bella S. Tawfik [26]. Each phase of the system's development for iris-based personal identification is introduced and described. Moment variations are a feature that writers employ for recognition. These four features are situated in the features area. There are two distinct classifiers used for classification: minimal distance using Euclidean distance and Mahalanobis distance. The system's final steps include feature extraction, pre-processing, and classification. The 180 unedited raw photos have been taken for data (three sets). One set is utilised for testing, and there are two sets totalling 120 iris photos. First, the photos are ready for feature extraction in this method. Following the computation of the four characteristics for each individual, the mean value for each individual is determined and placed in the features space.

The recognition rate for Mahalanobis distance is 100%. Kong [27] created a method that is independent of prior information and is derived from the geometric features of a convex polyhedral cone (e.g., iris images).

This study shows that an Iris Code template or one of its variations produces a convex polyhedral cone in a hyperspace. A straightforward approach that may be used in a single MATLAB command line to compute the centre ray, which is an approximate representation of the original biometric signal. The centre ray of an objective function on a collection of distributions is both an anticipated and an ideal ray. For testing the algorithms, authors employed one palm print database, two iris datasets UBIRIS.v1 and West Virginia University (WVU) iris databases. They only evaluated the red component of colour photographs because the iris texture is more distinct in this component. A real-time, reliable approach for detecting irises on faces with coronal axis rotation within the typical range of -40 to +40 was devised by C. Perez et al. [28]. This approach permits unrestricted head motions while looking at the background. The foundation of this technique is the use of anthropometric templates to identify the face and eyes. The elliptical form of faces and the placement of the lips, nose, and eyebrows are key characteristics employed by templates. A template that mimics the shape of the iris-sclera border is employed for iris detection. On five video sequences, the technique was contrasted with Maio-and Maltoni's Rowley's face detection approaches (TEST 1). Additionally, the technique was tested for iris identification in an additional batch of five video sequences (TEST 2). This technique was created in three steps, including iris detection, fine face detection, and coarse face detection.

It is preferred that the methods of engagement should be as natural as possible in order to improve the interaction in dynamic environments. A collection of permutations created by motions of the hand and arm might be used to characterize human hand gestures [29]. Depending on a variety of characteristics, gesture input may be divided into distinct groups [30]. Deictic gesture, which includes reaching for something or pointing towards something, is one of the types. Mimetic gestures refer to accepting or rejecting an action for an occasion. It is helpful for representing gestures in words. A gesture that defines an object or its qualities is called an iconic gesture. A hand gesture application in gallery browsing 3D depth data processing is presented by Chai et al. in their study [31]. The gesture framework was meant to integrate global structural information with local texture variation. In their study, Pavlovic et al. [32] came to the conclusion that in order to create an effective human computer interface, user gestures have to be rationally explicable. The aforementioned issues cannot currently be solved by gesture recognition technology in an acceptable manner. The complexity and robustness of the analysis and assessment for gesture recognition is one of the significant issues that have emerged throughout time. Different researchers have put forward and used various pragmatic gesture input methods for human computer interfaces. In their article [33], M. W. Mohanty and Yaqub took use of the online meeting platforms to effectively pinpoint and address security issues. To maintain user privacy and security, they deployed a photo resonance non-uniformity-based camera for digital authentication. For operating virtual games, Xu et al. [34] employed contact-based gadgets such accelerometer and EMG sensors. Numerous research have been done on hand motions, particularly gestures, by simulating the human body and building up a comprehensive body of information. It is now feasible to approach the problem from a mathematical perspective on the basis of that corpus of knowledge [35].

The limits of fingerprint, iris, and retina-based biometric person authentication were distinctly stated by the authors in [36]. The same may be said for person identification using signatures; some systems may compare visual representations of signatures, but the basis of a signature biometric system is behavioral, or how it is signed, rather than visual, or the image of the signature [37]. It indicates that because the attribute is behavioral in nature, it cannot be used to authenticate for a broad population and has limits when used with people with disabilities. Use of hand geometry is another potential biometric characteristic. For so-called one-to-many applications, in which a person is recognized solely by his biometric without any further identification, hand geometry is not appropriate in big populations [38]. There have also been suggestions for certain extreme biometric characteristics, such ear canal use. Researchers discovered that combining biometric features or using multimodality is one of the most promising strategies. Researchers in [24], using principal component analysis (PCA) on combined images of the face and ears, discovered that multi-modal identification performs significantly better than any individual biometric. Considering that we've already studied some of the most important biometric characteristics [39].

III. Recognition Techniques

A popular technical tool for confirming identity is biometric person identification [40]. It is extremely important for either domestic or global security. The majority of human body parts are unique, and some of the most prominent ones have been exploited to create automated identification verification systems. The display of a user's biometric characteristic within the framework of a certain system and application comprises both biological and behavioural components.

3.1 Iris Recognition

The chaotic morphogenetic processes that occur during embryonic development establish the visual texture of the human iris, which is thought to be unique for each individual and each eye [41]. The majority of people have employed the iris detection framework, which has been shown to be effective and persuasive in identifying a person with high accuracy and almost perfect matching. The procedure of taking a non-contact image of an iris often requires user involvement [42], both to guarantee that the iris is at a certain distance from the camera's focus plane in figure 1 and to register the iris image in the central imaging region. It is thought that the iris detection technique is very quick and accurate [43]. Iris recognition was first conceptualised on August 28, 1986, by Leonard Flom and Aran Safir, who then patented the method in a broad sense, preventing further advancement by the broader field until 1993, when they permitted John Daugman to create an algorithm for use, which was later patented in 1994. Iris recognition is mostly used for authentication and includes taking a high resolution photo of a subject's eye and comparing it to a data collection. Since they are chosen at random during gestation, the blood vessels in an iris are completely unique in the population. The technology is unable to confirm the component's viability, as is the case with many biometric approaches [44]. Iris recognition is a reliable method of identifying a person due to its stability and distinctiveness [45].

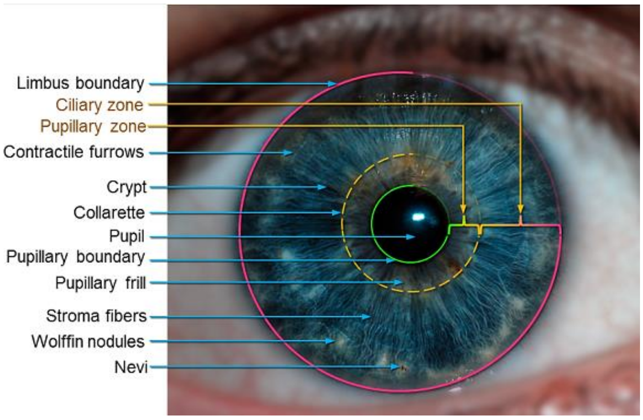

Figure 1. The Iris Recognition

3.2 Fingerprint Recognition

The biometric that has been investigated the most thoroughly is undoubtedly fingerprints. Fingerprints are one of the most often used ways for identifying people because of their distinctiveness, permanence, ease of collection, and modest size of the acquisition equipment (at least for electronic ones) [46]. Although fingerprint recognition has been practised since 1880, computerised fingerprint identification technologies are a considerably more recent development. Each person has a different finger and palm epidermis (skin). The hand is put on a sensing pad, which scans the ridges of the epidermis to be used as the characteristics indicated in figure 2, which is the most popular application of this technology for authentication. By taking a fingerprint off an object and scanning it into a computer, fingerprinting may also be utilised non-intrusively. In a recent development, the vitality of the appendage pressed onto the sensor can be assessed by detecting the perspiration between the ridges. This aids in preventing fake latex fingerprints and the use of high-resolution printed images of fingers, which still affect some less expensive systems [47].

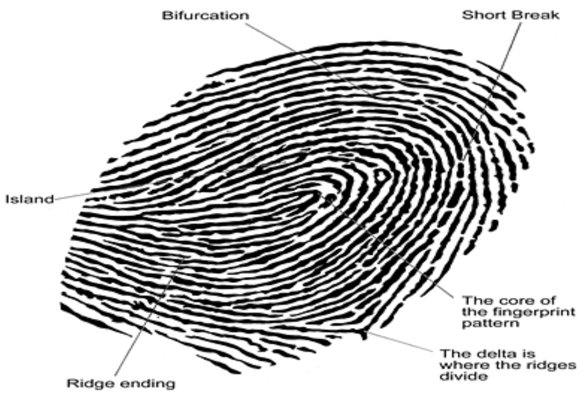

Figure 2. The Fingerprint Recognition

3.3 Hand Geometry Recognition

For authentication purpose, hand geometry biometric devices are gaining a lot of traction. Despite the fact that hand geometry is less distinctive than other biometrics (such as fingerprints) and has not been linked to criminal prosecution, it is a valid form of identification for the general population as seen in figure 3. Hand geometry has mostly been employed in person identification systems as a supplement to fingerprints. Geometric measurements and contour description are the two basic categories of hand geometry biometrics. It's a challenging error-pruned task to automatically extract geometric measures from a hand geometry photograph.

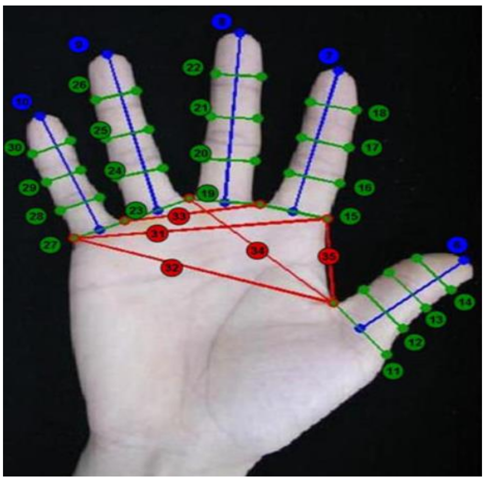

Figure 3. The Hand Geometry Recognition

The technique works better in a semi-automatic setting when a human user points out the key features of the hand's shape. The accuracy of contour description methods is often lower, but they are more reliable for automatic authentication processes [48]. Since more than 25 years ago, hand geometry recognition biometric devices have been employed for tasks including physical access and employee time/attendance. These technologies, which rely on the human hand's distinctive form, have withstood numerous ups and downs in the biometrics sector.

3.4 Palm Print Recognition

In addition to having a substantially bigger skin surface and other distinguishing features like primary lines, palm prints also share the majority of the distinguishing characteristics of fingerprints. Human hands have a pattern of ridges and valleys on their palms that resembles fingerprints in figure 4. Since the area of the palm is far greater than the area of a finger, palm prints should be even more recognisable than fingerprints. Palm print scanners are larger and more costly than fingerprint sensors since they need to record a larger area. Additionally, human palms have other distinguishing characteristics including main lines and wrinkles that may be photographed even with a cheaper, lower quality scanner [50]. Lastly, a very accurate biometric system may be created by combining all the characteristics of the palm, including hand geometry, ridge and valley features (such as minutiae and unique points like deltas), main lines, and wrinkles. Palm prints and fingerprints have been relied upon as a reliable means of identification for more than a century because of their uniqueness and longevity.

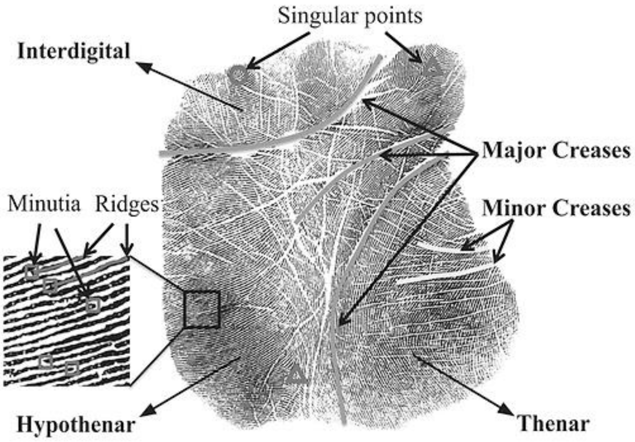

Figure 4. The Palm Print Recognition

3.5 DNA "Fingerprinting" Recognition

Every human cell has the well-known double helix structure known as DNA (deoxyribonucleic acid). A DNA sample is used to create a DNA profile or DNA fingerprint shown in figure 5. A (Adeline), C (Cytosine), G (Guanine), and T (Thymine) are the four teeth of a zipper that represents the molecular structure of DNA. Opposing teeth form one of two pairings, either A-T or G-C. The order of letters along the zipper determines the information in DNA [51]. This approach makes use of the biologically distinct DNA molecule patterns that exist between people. The DNA fragments' banding patterns display distinctive variations. In the United Kingdom, DNA prints were first used in 1983. The sole widespread application of DNA fingerprinting is to compare two samples to see if they are from the same person; it is not often utilised for authentication. Because so many people consider it to be an invasion of their privacy, it is not more widely used. Additionally, it requires a lot of calculation, which takes time to complete. The majority of people have distinct DNA, although monozygotic twins may not necessarily have unique DNA. Paternity testing and other forensic applications as well as criminal investigations all make use of DNA fingerprinting.

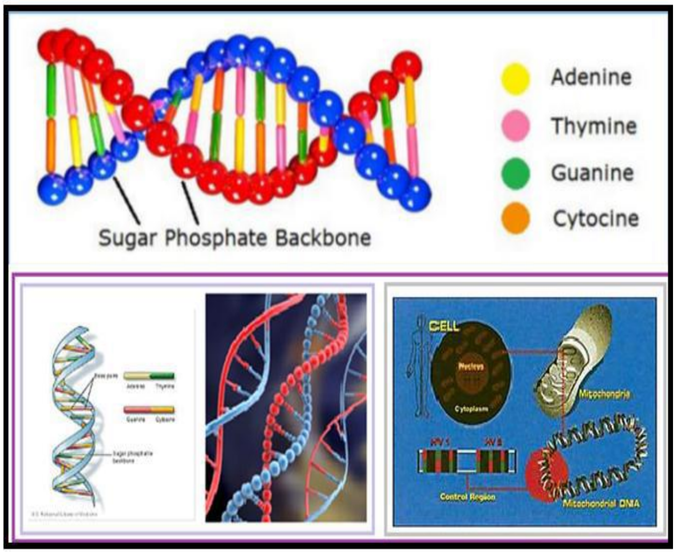

Figure 5. The DNA "Fingerprinting" Recognition

3.6 Signature Recognition

Signa-tures are behavioural biometrics that evolve over time and are influenced by the physical and emotional states of the signatories, making signature recognition a very difficult biometric recognition problem [6]. It is known that the way a person signs their name is a characteristic of that individual. Since we have always used signatures to authenticate all of our legal papers shown in figure 6, the concept is not new. Absolute signature validation, on the other hand, is a whole separate issue and is far more challenging. Some systems make use of pens that have pressure- and motion-sensing sensors. In this instance, force changes in the x and y directions are measured using a special pen that has a bi-axial accelerometer. The z-axis force's fluctuations are measured using a force sensor.

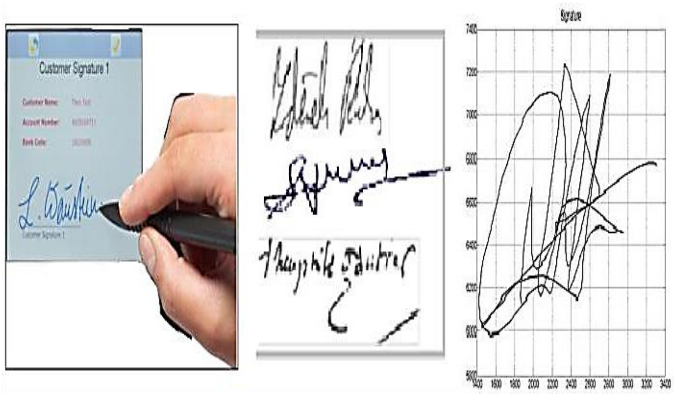

Figure 6. The Signature Recognition

An individual signs his or her name several times to register with the system. Each time a signature is made; the computer reads and examines the dynamic movements made by the signer. Software detects the actions of the pen and extracts important templates. Speed of signature, the sharpness of loops, and pressure fluctuations are a few examples. The profiles created by these templates are compared to profiles that are kept on the user's card or in a central database. A successful match verifies the user [52]. A signature verification process' goal is to validate or disprove the sample, but a signature recognition process' goal is to identify the author of a given sample.

3.7 Gait Recognition

Shakespeare is responsible for the invention of gait identification in his line, "Highest Queen of state, Great Juno arrives; I recognise her by her gait" [53]. Gait is a complicated spatio-temporal biometric that describes one's distinctive walking style shown in figure 7. Despite not being particularly unique, gait is enough of a differentiator to allow verification in some low-security applications. Gait is a behavioural biometric that may not be constant over time; especially if there have been significant changes in body weight, joint or brain traumas, or intoxication. Gait analysis is related to face image analysis, hence it could be a valid biometric. Gait-based systems are input-intensive and computationally expensive because they employ video sequence footage of a person walking to quantify a variety of motions at each articulating joint. This method has the advantage of allowing for remote identification on suitably low-resolution pictures. The method used to derive gait characteristics from the gait frames is quite straightforward and logical. There are several ways to approach this model-free methodology.

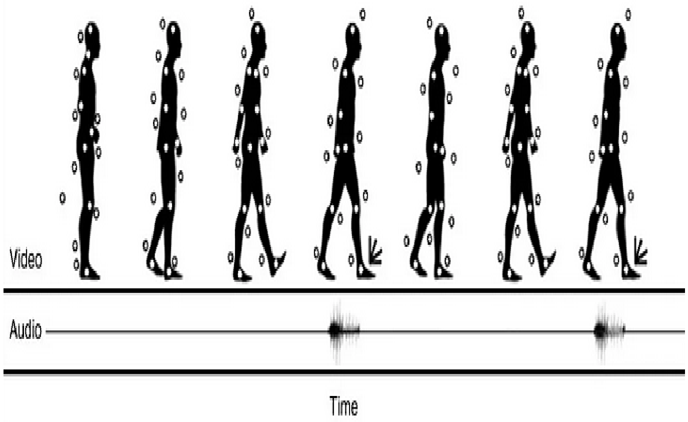

Figure 7. The Gait Recognition

3.8 Ear Recognition

One of the most distinctive physiological characteristics on the human body has been demonstrated to be the ear [54] shown in figure 8. They are quite immobile and maintain their form throughout life, which is what makes them so helpful for biometrics. However, ear biometrics may degrade significantly if the ears are covered by jewellery, hair, etc. There aren't any ear recognition systems in use right now. But there is a lot of contemporary study being done on the subject. The human ear is larger than the iris and fingerprint, and picture collection of the human ear is fairly straightforward and can be done from a distance, giving it certain benefits over other biometrics like iris, fingerprints, face, and retinal scans.

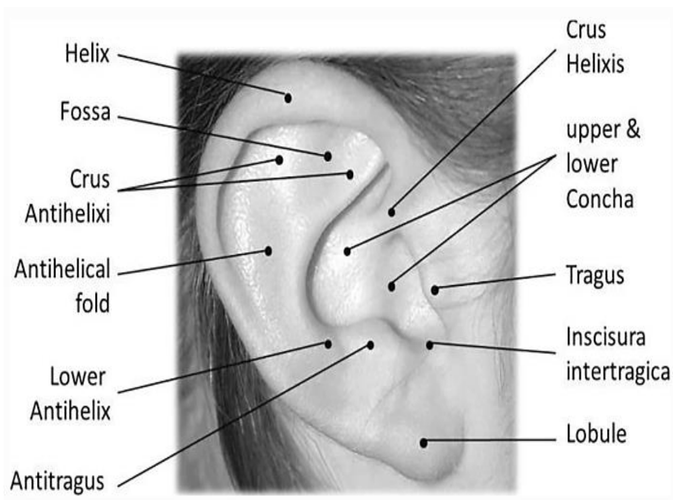

Figure 8. The Ear Recognition

3.9 Face Recognition

Because faces are one of the most frequent forms of identification that people employ in their visual contacts and because acquiring faces is non-intrusive, faces are one of the most widely accepted biometrics. In unattended authentication applications, face recognition raises concerns [55]. Face recognition software extracts facial features and recognises individual faces by looking for patterns, contours, and shadows on the face. All forms of facial processing, including tracking, detection, analysis, and synthesis, are included in the larger perspective. The most often used method is based on Eigen faces, which depict the differences between the face being recognised and the faces that have been registered in the database. The underlying mathematics for this face pattern recognition is principal component analysis with higher-order statistics. Using photographs of genuine faces [55].

3.10 Voice Recognition

Voice is a synthesis of behavioural and physiological biometrics [56]. The most practical biometric to employ is voice because that is how people naturally communicate. Additionally, speech may be used in a number of telephone-based or internet-based applications where other biometrics cannot be used and just requires modest equipment for capture. On some Sprint systems, voice recognition has already taken the place of keying in numbers. This type of voice recognition is comparable to speech recognition yet distinct from it. While speaker recognition technology confirms the speaker's identification, speech recognition technology translates what the speaker says [57]. Using a microphone, voice authentication or speaker recognition captures a person's voice. The digitalized voice from the captured recording is utilised for authentication. The user can either speak or enunciate a known text to acquire the speech (text dependant) (text independent). Based on the utterance of a specific, prepared phrase, a text-dependent speech recognition system works. A speech recognition system that is not dependent on text can identify the speaker regardless of what she says. Though more challenging to build than a text-dependent system, a text-independent system provides more fraud protection [58]. To create a voice template, the collected speech is then improved and its distinctive qualities are retrieved. Stochastic templates and model templates are the two different categories of templates. A measure of the likelihood of the observation given the template is produced by stochastic templates and requires probabilistic matching techniques like the well-known Hidden Markov Model. The matching methods applied to model templates are deterministic. It is expected that, with some distortion, the observation and the model are comparable. When the observation and model are aligned, the minimal error distance is measured to determine the matching result. The Nearest Neighbours algorithm, Vector Quantization, and Dynamic Time Warping algorithm are some of the matching methods frequently used for model templates.

3.11 Odor Recognition

Each thing is known to have an odour that is distinctive of its chemical makeup, and this might be used to identify between different objects. An array of chemical sensors, each sensitive to a certain set of (aromatic) molecules, are exposed to a whiff of air surrounding an item [59]. An individual can be recognised by a specific element of the smell released by the body of a human (or any animal). Despite the odours of deodorants and the shifting chemical makeup of the surroundings, it is unclear if variations in body odour may be noticed. A recent advancement in biometrics is odour recognition. The nasal sensory apparatus is extremely sensitive to even the slightest variations in fragrance, and human scents are reportedly unique. The technology needed to create a system that can imitate the human nose and recognise objects by scent is still rather advanced.

3.12 Keystroke Recognition

It is assumed that every keyboard user has a unique typing style. Although this behavioural biometric is not anticipated to be specific to each person, it does provide enough discriminating data to enable identification verification [60]. Keystroke dynamics is a behavioural biometric, thus it's possible to anticipate seeing significant variances in certain people's regular typing habits. Furthermore, while someone types information into a system, their keystrokes might be covertly observed shown in figure 9. Many researchers might not find the type dynamics interesting for identification. However, research has shown that the two factors dwell time, the length of time a key is held down, and flight time, the amount of time that passes between releasing a key and pressing the one after it, also known as inter-character timing can provide 99% accurate identification of the person who is typing. The time it takes to identify the appropriate key, the flight time, and the residence time all contribute to how differently each person types on a keyboard. The pace and rhythm of typing can also change. Keystroke recognition falls into two categories. Static, one-time recognition at the start of the engagement and Continuous, recognition as the interaction continues.

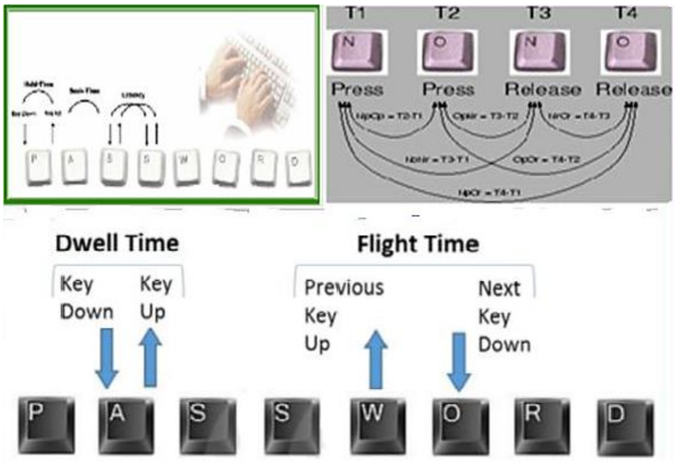

Figure 9. The Keystroke Recognition

IV. Comparison of Commonly Used Recognition Techniques

This section provides a summary of the current state of the art for the various biometric modalities based on the following parameters: error rates, inter-session variability, universality, noise sensitivity, architectural features like the viability of distributed template storage, sensor cost, vendor choice, pre-existing smartcard match-on-card implementations, and susceptibility to covert acquisition. To the best of our ability, we categories each attribute as low (A), medium (A+), or high (A++), and we provide the findings shown in table 1. At least twelve biometric methods are currently commercially accessible, and others are in the research and development stages [61]. Furthermore, although there hasn't been much research on this, a modality itself could have flaws even if some of the drawbacks could be fixed [62]. However, factors other than matching performance must be taken into account when selecting a biometric feature for a certain application.

• **Generality :-** Every person who uses the programme should have this quality.

• **Exclusiveness :-** The population as a whole should differ enough from the supplied feature.

• **Stability :-** A person's biometric feature should be sufficiently stable over time in relation to a certain matching algorithm. A characteristic that fluctuates considerably is not a good biometric.

• **Quantifiable :-** The biometric attribute should be able to be collected and digitally stored using appropriate tools without causing the subject undue hardship. Additionally, analyzing the collected raw data to derive representative characteristics should be possible.

• **Effectiveness :-** The recognition performance [63] and the resources needed to get that accuracy should satisfy the application's needs.

• **Respectability :-** Users of the application from the target audience should be willing to provide the system access to their biometric characteristic.

• **Contrivance :-** The application's security requirements should take into account how easily a biometric characteristic may be replicated using artifacts, such as false fingers in the case of physical traits and mimicry in the case of behavioral traits.

Table 1. The Comparison of Commonly Used Recognition Techniques

Biometrics	Generality	Exclusiveness	Stability	Quantifiable	Effectiveness	Respectability	Contrivance
Iris Recognition	A++	A++	A++	A+	A++	A	A++
Fingerprint Recognition	A+	A++	A++	A+	A++	A+	A++
Hand Geometry Recognition	A+	A+	A+	A++	A+	A+	A+
Palm Print Recognition	A+	A++	A+	A++	A++	A+	A+
DNA Fingerprinting Recognition	A++	A++	A++	A	A++	A	A
Signature Recognition	A	A	A	A++	A	A++	A
Gait Recognition	A+	A	A	A++	A	A++	A+
Ear Recognition	A+	A+	A++	A+	A+	A++	A+
Face Recognition	A++	A	A+	A++	A	A++	A
Voice Recognition	A+	A	A	A+	A	A++	A
Odor Recognition	A++	A++	A++	A	A	A+	A
Keystroke Recognition	A	A	A	A+	A	A+	A+

V. Biometric Databases System

If biometric technology is properly applied to strengthen security systems worldwide, it might have a significant positive influence on society. This would make it easier to deal with the escalating instances of terrorism, criminality, and fraud. However, because biometrics gives governments and businesses access to a vast quantity of personal data about people, they run the risk of hurting society. This section covers the use of biometric databases.

5.1 MUCT Database

The 3755 faces in the MUCT database have 76 manual markers. The database was developed in order to offer greater variety in lighting, age, and ethnicity than the existing landmarked 2D face datasets. Milborrow / University of Cape Town is known by the initials MUCT. In December 2008, a sample of the database's participants was taken from residents near the University of Cape Town campus's Leslie Social Sciences Building [64]. Students, parents attending graduation ceremonies, high school instructors attending a conference, and university staff members including cleaners and security guards were among this eclectic group of people. About equally many men and women, people of all ages and colors, and a broad variety of things were photographed. One of the researchers went door-to-door to ask individuals whether they would agree to be photographed in exchange for a chocolate bar in order to gather subjects. If the subjects were wearing makeup, spectacles, or headpieces, they kept them on for the photos. Subjects weren't instructed to make any certain facial expressions, thus in reality, most people were captured grinning or keeping their faces neutral. Each subject was at least 18 years old.

5.2 XM2VTS Database

Synchronized video and voice data from 295 people were collected during four sessions that were separated by one month and are available in the XM2VTS database. Two recordings, one of a speech shot and the other of a head shot, were recorded for each session. Each subject's frontal face and voice were recorded during the recital of a sentence for the speech shot. Three sets a training set, an evaluation set, and a test set make up the database [65]. The evaluation set (LP Eval) was used to calculate the decision thresholds (as well as other hyper-parameters) needed by classifiers, whilst the training set (LP Train) was used to construct client models. In order to estimate the performance, the test set (LP Test) was employed. 200 customers, 25 evaluation impostors, and 70 test impostors made up the 295 subjects. The training and assessment sets can be divided into two alternative configurations or partitioning strategies. They are referred to as LP1 and LP2 in this publication and are known as the Lausanne

Protocol I and II. The test set is the same in both situations. There are three training photos for LP1 and four training pictures for LP2, which is where they diverge.

5.3 VidTIMIT Database

The 43 persons who are included in the video and audio recordings that make up the VidTIMIT dataset may be seen repeating simple words. Research on subjects like automated lip reading, multi-view face recognition, multi-modal voice recognition, and person identification may benefit from it [66]. The dataset was collected over the course of three sessions, with an average gap of seven days between Sessions 1 and 2 and six days between Sessions 2 and 3. The sentences were from the TIMIT corpus' test section. Each individual has ten sentences. The first session is designated to the first six sentences, which are arranged alphabetically by filename. The following two phrases belong in Session 2, and the final two in Session 3.

5.4 BilVidco Database

For queries on low-level (colour, shape, and texture) spatiotemporal, semantic, and semantically based aspects on video data, BilVideo offers integrated support [67]. Any number of directional, topological, object-appearance, 3D relation, trajectory-projection, and similarity-based object-trajectory criteria may be included in a spatio-temporal query. While an object-relational database manages queries on semantic and low-level aspects, BilVideo uses a knowledge-base, which is made up of a fact-base and a complete set of rules, to handle spatio-temporal queries. The knowledge base and object-relational database are both involved in the query processor's interactions with them in order to reply to user questions that combine spatiotemporal, semantic, and low-level feature query requirements. The query processor smoothly integrates intermediate query results generated from these system elements and sends them to Web clients. Additionally, users have access to a text-based SQL-like query language and can browse the video collection before submitting complicated and detailed searches [68]. BilVideo is application-independent since it supports any application with query needs on spatio-temporal, semantic, and low-level properties on video data. Through the development of external predicates enabled by its query language, it may be readily customised to meet the unique requirements of such applications without much work or performance loss.

5.5 BANCA Database

For training and testing multi-modal verification systems, the BANCA database is a brand-new, sizable, realistic, and difficult multi-modal database. The BANCA database was recorded in two modalities [69] and four European languages (face and voice). Both high-quality and low-quality mics and cameras were employed for the recording. Over the course of 12 sessions spread over three months, the patients were observed in the three separate settings of controlled, degraded, and unfavorable. Half males and half women out of the total 208 individuals detained were men. In order to evaluate multi-modal identity authentication with numerous acquisition devices (2 cameras and 2 microphones) and under diverse circumstances, the BANCA (biometric access control for networked and e-commerce applications) database [70] was created (controlled, degraded and adverse). A total of 260 participants, or 52 people (26 males and 26 females), had their video and voice data recorded for 5 distinct languages (English, French, German, Italian, and Spanish). Each population was separated into two groups of 13 participants, one for each gender and language (denoted g1 and g2). Each participant took part in 12 recording sessions, with each session including two records: one documenting real client access (T) and the other documenting an educated imposter assault (I). There are 5 photos per record in the database's picture section. Three distinct situations were created from the 12 sessions.

VI. Benefits, Drawbacks and Applications of Biometrics Approaches

For thousands of years, people have utilized physical traits including the face, voice, and movement to identify one another. A biometric is a strong, recognizable, quantifiable physical or behavioral attribute of an individual that is used to establish that person's identification [71]. Any biometric feature should be distinct, readily convertible, and prone to fewer changes over time. One biometric feature that differs from person to person is the voice. In a similar vein, iris doesn't alter over time. Pattern recognition systems are the foundation of the biometric systems. A biometric system functions by gathering biometric data [72] from a person, extracting a feature set from the data [73], and comparing the feature set to the template set in the database. It is essentially a pattern recognition system. Below table 2, we explore the benefits, drawbacks, and applications of biometrics approaches in this section.

Table 2. The Benefits, Drawbacks and Applications of Biometrics Approaches

Biometrics Approaches	Benefits	Drawbacks	Applications
Iris Recognition	• Very precise (Iris pattern matches 1 in 10 billion people). • Extremely scalable. • The use of contact lenses or spectacles has no impact on accuracy. • Avoid touching the system directly. • Processing speed is promising due to the small template size (2 to 5 seconds). • Low false acceptance rate, lifelong stability. • High levels of randomization, high levels of protection. • Tractability of encoding and decision-making.	• Relatively pricy. • The scanner can be fooled by high-quality photographs • Accurate scanning requires user assistance. • Less user convenience due to user's immobility throughout scanning process. • Less market competition, obscured by eyelashes, glasses, or reflections • Illumination should not be noticeable or bright. • Long distances should be difficult. • Vulnerable to poor image Quality. • The iris might change as a re of diabetes or other major illnesses.	• Recognition (Adhaar card in India). • Access Management (Google uses for their data centers). • Security at home (land, air and sea ports of entry of UAE).

Fingerprint Recognition	• The most recent technology. • Relatively affordable. • More dependable and very secure. • Due to the minimal template size, matching is quick. • Less memory is used. • The most popular technology. • High degree of precision. • Multiple fingers may be registered. • A variety of deployment contexts. • They are not obtrusive and do not alter organically.	• Cuts, scars, or the lack of a finger might be a barrier to identification. • Easily tricked by a wax-based fake finger. • Is in close proximity to the system. • Demands substantial computational resources. • Worn out or subject to alterations with time. • Some persons have damaged or removed fingerprints. • Exposed to noise and distortion as a result of dirt and twisting.	• Validation of a Driver's License • Visa issuance and border control. • Organizational access control. • Law enforcement forensics.
Hand Geometry Recognition	• The outcome is unaffected by changes in skin moisture or texture. • It is also user-friendly and long-lasting. • The compact template size and ease of usage. • Non-intrusive. • Operable under demanding and difficult conditions. • Reliable and established technology. • Low rate of failure to enrol (FTE).	• Inaccurate and not particular. • Only adults may use it effectiv • FAR (false acceptance rate) and FRR (false rejection rate) are relatively high. • Wearing jewellery may provid scanning hurdle. • Results are not accurate yet. • Not yet developed. • Rather expensive. • Hand injuries may hinder the system from functioning correctly.	• Nuclear energy facilities. • Control of military access.
Palm Print Recognition	• Compared to fingerprints, more distinguishing traits may be recorded. • More effective than fingerprints in identifying systems.	• Variations in light and distortions in an uncontrolled environment. • Scanners are larger and more costly. • Recognition issues for low quality photos.	• Identification of the individual. • Medical diagnosis. • Blood connection information. • Aathlete selection.

	• Better recognition with low resolution cameras and scanners. • More durable and dependable.		
DNA Fingerprinting Recognition	• The likelihood of two people having the identical DNA profile is less than one in a hundred billion. • It offers the highest level of accuracy.	• Getting the desired outcome requires a lengthy process of sample acquisition. • There are privacy concerns ev if it provides more informatio • There should be more storage space. • Sampling contamination or sample deterioration has an impact on the outcome. • Expensive and inconvenient. • Very slow processing time. • No real-time matching. • Intrusive - requires physical sample collection.	• Establishing innocence or guilt. • Network and physical security.
Signature Recognition	• No two signatures are alike. • It is suitable for a large number of commercial transactions. • It has a low false acceptance rate (FAR), is non-intrusive, and has a respectable accuracy rate. • Have no problems with privacy rights. • The template may be easily restored if it is taken.	• there is a change in behaviour during signing, there is a chance that the live sample template will change. • The user must be comfortable with using the signing tablet. • Professionals can fake signatures to trick the system. • Has a very small market. • Signature changes over time. • Same person can have inconsistent signatures.	• Authentication and authorisation. • Banking Methods (The Chase Manhattan Bank, Chicago, the First bank using Signature System).
Gait Recognition	• It doesn't do any harm. • Convenient in use. • Easily obtained from a distance.	• Lack of total precision. • Reliability. • Lack of temporal invariance.	• Comparative biomechanics. • Forensic scienc. • Medical diagnostics. • Chiropractic.

	• Used to identify medical illnesses (recording changes in walking patterns - Parkinson's disease).	• High computational cost due to the increased number of computations.	• Osteopathic use.
Ear Recognition	• Faster identification. • More stable. • Less computing complexity. • Fixed form and appearance. • Shorter processing time	• Recognition errors due to imperfect visuals. • Imprecise identification owing to the impact of jewellery, headgear, and hairstyles. • Not thought to be particularly unique	• Surveillance. • Law enforcement forensics.
Face Recognition	• Completely non-intrusive, meaning it doesn't entail physical touch. • Database storage of templates is simple. • Accepted by society. • Simplified statistics for identifying faces in images. • Comparable to the human authentication procedure. • Practicality and advanced technology. • Cameras, which are now employed for taking images, can be utilised. • Quicker identification time.	• In the case of twins, uniqueness is not certain. • Facial characteristics alter over time or vary. • Variable expressions may have an impact on the accuracy of recognition. • For accurate input, lighting is quite important. • Most individuals find privacy invasions unsettling. • More suited for authentication. • Limited information in 2D. • Stable to light, orientation, and facial expressions. • Unusable while wearing a mask or other face-covering veils. • More suitable for authentication.	• Verification of Identity. • Verification of Access Control. • Human-computer interaction. • Identification of criminals. • Monitoring.
Voice Recognition	• No additional new devices are required. • It is simple to implement. • Low cost. • Convenience. • Intrusiveness are all advantages.	• Subject to noise and microphone quality. • Accuracy may be impacted by severe sickness or throat issues. • Easily spoof able. • High rate of erroneous non-matches.	• Online transactions. • Banking and healthcare systems that use interactive voice response. • Audio signatures on papers that are digital.

		• Significantly decreased performance as a result of input system-related issues.	• Amusement and rescue services. • Systems for online education.
Odor Recognition	• By identifying the components of the combination, a mixture of scents may be identified.	• There are still no applications on file. • Quantification senses are challenging. • It is not pleasant for artificial to do all tasks. • The distinctiveness of deodorants and fragrances is diminished.	• Forensics in Law Enforcement. • Observation.
Keystroke Recognition	• Identification is quick and secure, requires nothing in the way of additional hardware or sensors, and is inexpensive. • There is no need to be concerned about being observed when typing. • There is no need for training in order to enrol or register their live samples.	• Conditions like illnesses, day gaps, keyboard changes, etc. might alter the rhythm of typing. • This is a young technology. • There is no bias-based information. • Less user convenience.	• A mechanism of authentication. • System for multifactor authentication. • Monitoring system.

VII. Constraints

The following restrictions apply to biometric systems that use a single biometric trait.

7.1 Error in the Sensed Data

Data that was felt might be noisy or corrupted. Examples of noisy data include a scarred fingerprint or a voice that has been affected by cold. Noisy data may also be the consequence of damaged or poorly maintained sensors (such as a fingerprint sensor that has accumulated dirt) [74] or adverse environmental factors (such as inadequate lighting for a user's face in a face recognition system) [75]. A user may be wrongly denied if noisy biometric data is erroneously matched with database templates.

7.2 Within-Class Changes

The matching process may be impacted by the fact that the biometric data collected from a person during authentication [76] may be significantly different from the data used to create the template during registration. When sensor properties are changed (for example, by switching sensors, the sensor interoperability problem), this variance is often brought on by a user who is inappropriately using the sensor or during the verification step. Another illustration is how a person's changing psychological composition may cause them to exhibit radically diverse behavioural tendencies over time incidents.

7.3 Individuality

Although a biometric property is anticipated to vary widely between people, the feature sets utilised to describe these features may share a lot of commonalities between classes. This restriction limits the biometric trait's capacity to discriminate. In two of the most widely used representations of hand geometry and face, Golfarelli et al. [77] have demonstrated that the information content (number of identifiable patterns) is only of the order of and, respectively. Each biometric feature therefore has a theoretical upper limit on how well it can discriminate.

7.4 Lack of Universality

Although it is believed that every user will have the acquired biometric feature, it is really feasible. The biometric system is affected by noisy photos. (a) Getting a fingerprint a user's input during enrolment. (b) A user's fingerprint [78] that was collected three months later during verification. The appearance of scars or wounds may lead to inaccurate fingerprint matching outcomes. For a portion of users to lack a specific biometric. Because of the subpar quality of the ridges, a fingerprint biometric system, for instance, could be unable to extract characteristics from the prints of some people. As a result, utilising a single biometric feature is related with a rate of failure to enrol (FTE). According to empirical estimates, up to 4% of the population may have poor-quality fingerprint ridges that are challenging to scan with the fingerprint sensors that are already on the market and cause FTE mistakes. In a speaker recognition system, the FTE issue is reported by Den Os et al. [79].

7.5 Spoof Assaults

To get around the system, a fraudster can try to impersonate a legitimately registered user's biometric characteristic. This kind of assault is particularly pertinent when behavioural characteristics like voice and signature are employed. However, spoof attacks [80] can also target physical characteristics. For instance, it has been shown that it is feasible to create false fingers or fingerprints in a fair amount of time to get around a fingerprint verification system, despite the fact that doing so is difficult, time-consuming, and requires the assistance of a real user.

VIII. CONCLUSION

A single parameter is not enough to enforce security. In order to create a safe environment, various dimensions of crucial check points must be considered instead of one-dimensional issue solving. Several settings offer secure authentication. An individual's security token, such as a physical key or a smart card, is one of the parameters. If biometric technology is properly applied to strengthen security systems worldwide, it might have a significant positive influence on society. This would make it easier to deal with the escalating instances of terrorism, criminality, and fraud. However, because biometrics gives governments and businesses access to a vast quantity of personal data about people, they run the risk of hurting society. In current technological age, biometrics, which refers to the examination of biological data gains major relevance. This paper's main goal is to give a chronological overview of various recognition techniques, their applications, benefits, drawbacks, and constraints. Automated systems will need to be able to identify people with a very high degree of certainty in real time and in the near future. Biometrics is already widely used in smart mobile devices, which significantly boosts their adoption. Continuous and many modality automatic authentication techniques are chosen for the best progress and future.

IX. REFERENCES

[1]. Y Tian, "Artificial Intelligence Image Recognition Method Based on Convolutional Neural Network

Algorithm[J]", IEEE Access, vol. PP, no. 99, pp. 1-1, 2020

[2]. Ali Mir Arif Mir Asif , Shaikh Abdul Hannan, Dr. Yusuf Perwej, Mane Arjun Vithalrao, “An Overview and Applications of Optical Character Recognition”, Journal of Advance Research In Science And Engineering (IJARSE), India, ISSN 2319-8346 (P), ISSN-2319-8354(E), Volume 3, Issue 7, Pages 261- 274, 2014

[3]. Aparna Trivedi, Chandan Mani Tripathi, Dr. Yusuf Perwej, Ashish Kumar Srivastava, Neha Kulshrestha, “Face Recognition Based Automated Attendance Management System” , International Journal of Scientific Research in Science and Technology(IJSRST), Volume 9, Issue 1, Pages 261-268, 2022, DOI: 10.32628/IJSRST229147

[4]. Sharkas, M. Abou Elenien, Eigenfaces vs. Fisherfaces vs. ICA for Face Recognition; A Comparative Study, 9th International Conference on Signal Processing, 2008, ICSP 2008., pp.914919, 2008

[5]. F. Ozgul, C. Atzenbeck, A. Celik and Z. Erdem, "Incorporating data sources and methodologies for crime data mining", Intelligence and Security Informatics (ISI) 2011 IEEE International Conf., pp. 176-180, 2011

[6]. Yusuf Perwej, Shaikh Abdul Hannan, Nikhat Akhtar, “The State-of-the-Art Handwritten Recognition of Arabic Script Using Simplified Fuzzy ARTMAP and Hidden Markov Models”, International Journal of Computer Science and Telecommunications (IJCST), Sysbase Solution (Ltd), UK, London, ISSN 2047-3338, Issue 8, Pages 26 - 32, 2014

[7]. Jung-Hoon Lee, Kyeongrok Kim, Jae-Hyun Kim, "Design of CycleGAN model for SAR image colorization", 2021 IEEE VTS 17th Asia Pacific Wireless Communications Symposium (APWCS), pp.1-5, 2021

[8]. L. Ma, T. Tan, Y. Wang, and D. Zhang, “Efficient iris recognition by characterizing key local variations,” IEEE Trans. Image Process., vol. 13, pp. 739–750, 2004.

[9]. Yusuf Perwej, Nikhat Akhtar, Firoj Parwej, “The Kingdom of Saudi Arabia Vehicle License Plate Recognition using Learning Vector Quantization Artificial Neural Network”, International Journal of Computer Applications (IJCA), USA, ISSN 0975 – 8887, Volume 98, No.11, Pages 32 – 38, July 2014, DOI: 10.5120/17230-7556

[10]. Parwej D. 2013. The state of the art recognize in arabic script through combination of online and offline. International Journal of Computer Science and Telecommunications, 4(3): 60-66, 2013

[11]. Parwej, F.: English sentence recognition using artificial neural network through mouse-based gestures. arXiv preprint arXiv:1301.4659 , 2013

[12]. Dipietro, L.; Sabatini, A.M.; Member, S.; Dario, P. A survey of glove-based systems and their applic.. IEEE Trans. Syst. Man Cybern. Part C Appl. Rev, 38, 461–482, 2008

[13]. Yusuf Perwej, Firoj Parwej, “Perceptual Evolution of Playout Buffer Algorithm for Enhancing Perceived Quality of Voice Transmission over IP”, International Journal of Mobile Network Communications & Telematics (IJMNCT), Academy & Industry Research Collaboration Center (AIRCC), USA, Volume 2, No. 2, Pages 1-19, 2012, DOI: 10.5121/ijmnct.2012.2201

[14]. P. V. Benos, A. S. Lapedes and Gary D. Stormo, "Is there a code for protein-DNA recognition? Probab(ilistical)ly?", BioEssays, vol. 24, pp. 466-475, 2002

[15]. K. Yanai and Y. Kawano, "Food image recognition using deep convolutional network with pre-training and fine-tuning", 2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), pp. 1-6, 2015

[16]. Deshpande, N. T., & Ravishankar, S., Face Detection and Recognition using Viola-Jones algorithm and Fusion of PCA and ANN. Advances in Computational Sciences and Technology, 10(5), 1173- 1189, 2017

[17]. Firoj P An empirical evaluation of off-line Arabic handwriting and printed characters recognition system. Int J Comput Sci, (9), 2012

[18]. Bakhshi, Y., Kaur, S. and Verma, P.,. An Improvement in Face Recognition for Invariant Faces. 6(2), pp. 423-426, 2016

[19]. Poon, B., Amin, M.A. and Yan, H., 2016. Improved Methods on PCA Based Human Face Recognition for Distorted Images. In Proceedings of the International MultiConference of Engineers and Computer Scientists (1).

[20]. Siswanto, Adrian Rhesa Septian, Anto Satriyo Nugroho, and Maulahikmah Galinium. "Implementation of face recognition algorithm for biometrics based time attendance system." 2014 International Conference on ICT For Smart Society (ICISS). IEEE, 2014.

[21]. Lukas, Samuel, et al. "Student attendance system in classroom using face recognition technique." 2016 Information and Communication Technology Convergence (ICTC). IEEE, 2016.

[22]. Yusuf Perwej , Firoj Parwej, Asif Perwej, "Copyright Protection of Digital Images Using Robust Watermarking Based on Joint DLT and DWT ", International Journal of Scientific & Engineering Research (IJSER), France, ISSN 2229-5518, Volume 3, Issue 6, Pages 1- 9, 2012

[23]. Yusuf Perwej, Asif Perwej, Firoj Parwej, "An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection", International journal of Multimedia & Its Applications (IJMA), Academy & Industry Research Collaboration Center (AIRCC) , USA , Volume 4, No.2, Pages 21- 38, 2012, DOI: 10.5121/ijma.2012.4202

[24]. Asif Perwej, Dr. Yusuf Perwej, Nikhat Akhtar, and Firoj Parwej, "A FLANN and RBF with PSO Viewpoint to Identify a Model for Competent Forecasting Bombay Stock Exchange", COMPUSOFT, SCOPUS, International Journal of Advanced Computer Technology, 4 (1), Volume-IV, Issue-I, Pages 1454-1461, 2015, DOI: 10.6084/ijact.v4i1.60

[25]. A. Radman, K. Jumari, N. Zainal,' Fast and reliable iris segmentation algorithm', IET Image Process.,Vol.7, Iss. 1, pp. 42–49, 2013.

[26]. E. Elfakhrany,Ben Bella S. Tawfik 'IRIS Recognition using Conventional Approach' IEEE 9th international colloquium on signal processing and its applications, pp-89-94,8 - 10 mac., Kuala Lumpur, Malaysia, 2013

[27]. Adams Wai-Kin Kong ,'Modeling IrisCode and Its Variants as Convex Polyhedral Cones and Its Security Implications IEEE Transactions On Image Processing, Vol. 22, No. 3,pp- 1148-1160, March 2013.

[28]. Claudio A. Perez, Vanel A. Lazcano, and Pablo A. Estevez, 'Real-Time Iris Detection on Coronal-Axis-Rotated Faces', IEEE Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews,Pp-971-978, Vol. 37, No. 5, September 2007 .

[29]. Krevelen, D. W. F. V., Poelman, R. A Survey of Augmented Reality Technologies, applications and limitation. The Int. Journal of Virtual Reality, vol. 9 9(2), 2010, pp. 1-20.

[30]. Mitra, S., Acharya, T., Gesture Recognition: A survey. IEEE Transactions on Systems. Man and Cybernetics (SMC) - Part C: App. and Reviews, vol. 37(3), 2007, pp. 211-324.

[31]. Chai, Xiujuan, Kongqiao Yikai, Wang, Fang. Robust hand gesture analysis and application in gallery browsing. In Proceeding of ICME, New York, 2009, pp. 938-94.

[32]. Pavlovic, V., Sharma, R., Huang, T.S. Visual interpretation of hand gestures for human-computer interaction: A review. IEEE Trans. on Pattern Analysis and Machine Intelligence (PAMI), vol. 7(19), , 1997, pp. 677–695.

[33]. M. Mohanty and W. Yaqub, "Seamless authentication for online teaching and meeting," 2020 IEEE Sixth International Conf.on Multimedia Big Data (BigMM), 2020, pp. 120-124.

[34]. Xu, Z., Xiang, C., Wen-hui, W. Ji-hai,, Y., Lantz, V., Kong-qiao, W. Hand Gesture Recognition and Virtual Game Control Based on 3D Accelerometer and EMG Sensors. In Proceedings of IUI'09, , 2009, pp. 401-406.

[35]. Lee, C. S., Ghyme, S. W., Park, C. J., Wohn. K. The Control of avatar motion using hand gesture. In

Proc. of Virtual Reality Software and tech. (VRST), 1998, pp. 59-65.

[36]. S. Bengio and J. Mariethoz, Biometric Person Authentication IS A Multiple Classifier Problem, Google Inc, Mountain View, CA, USA, , IDIAP Research Institute, Martigny, Switzerland

[37]. Biometric technology, Hand Geometry Identification Technology, www.biometricvision.com

[38]. L. Yuan, Z. Mu, and Z. Xu, Using Ear Biometrics for Personal Recognition, School of Information Engineering, Univ. of Science and Technology Beijing. Beijing 100083

[39]. Yusuf Perwej, Dr. Ashish Chaturvedi, "Machine Recognition of Hand Written Characters using Neural Networks", International Journal of Computer Applications (IJCA), USA, ISSN 0975 – 8887, Volume 14, No. 2, Pages 6- 9, 2011, DOI: 10.5120/1819-2380

[40]. K. L. Kabir et al., "Projection-based features: A superior domain for handwritten Bangla basic characters recognition", 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO), pp. 1-7, 2015

[41]. Li, "An Iris Recognition Algorithm Based on Coarse and Fine Location", IEEE 2nd international conference on Big Data Analysis, 2017

[42]. F. C. Soon, H. Y. Khaw, J. H. Chuah and J. Kanesan, "PCANet Based Convolutional Neural Network Architecture For Vehicle Model Recognition System", IEEE Tran. on Intelligent Transp. Systems, vol. PP, no. 99, pp. 1-11, 2018

[43]. P. Jonathon Phillips, Alvin Martin and C.L. Wilson Mark Przybocki, An Introduction to Evaluating Biometric Systems, National Institute of Standards and Technology, 2000 IEEE.

[44]. Ivor Simpson, biometrics: issues and applications, 6th Annual Multimedia Systems, Electronics and Computer Science, University of Southampton 2006.

[45]. Yusuf Perwej, Dr. Ashish Chaturvedi, "Neural Networks for Handwritten English Alphabet Recognition", International Journal of Computer Applications (IJCA), USA, ISSN 0975 – 8887, Volume 20, No. 7, Pages 1- 5, 2011, DOI: 10.5120/2449-2824

[46]. Kai Cao and Anil K Jain, "Fingerprint indexing and matching: An integrated approach", 2017 IEEE International Joint Conference on Biometrics (IJCB), pp. 437-445, 2017

[47]. Wang Yuan, Yao Lixiu and Zhou Fuqiang, "A real time fingerprint recognition system based on novel fingerprint matching strategy", 2007 8th International Conference on Electronic Measurement and Instruments, pp. 1-81, 2007

[48]. S. Ribaric and I. Fratric, "A Biometric Identification System Based on Eigen Palm and Eigen Finger Features", IEEE Transaction on pattern analysis and machine intelligence, vol. 27, no. 11, pp. 1698-1709, 2005

[49]. Yusuf Perwej, "Recurrent Neural Network Method in Arabic Words Recognition System", for published in the International Journal of Computer Science and Telecommunications (IJCST), Sysbase Solution (Ltd), UK, London, ISSN 2047-3338, Volume 3, Issue 11, Pages 43-48, November 2012

[50]. Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE transactions on circuits and systems for video technology, vol. 14, no. 1, january 2004

[51]. Betch, D. "DNA Fingerprint in Human Health and Society" Biotechnology Information Series (Bio-6)

[52]. Kevin Daimi and Katherine Snyder, "Security Requirements forMultimodal Biometric Systems", Department of Mathematics and Computer Science, University of Detroit Mercy, Detroit, Michigan 48219, USA

[53]. Nikolaos V. Boulgouris, Dimitrios Hatzinakos and Konstantinos N. Plataniotis, "Gait Recognition: A challenging signal processing technology for biometric identification", IEEE signal processing magazine, 2005

[54]. Yusuf Perwej, "Unsupervised Feature Learning for Text Pattern Analysis with Emotional Data Collection: A Novel System for Big Data Analytics", IEEE International Conference on Advanced computing Technologies & Applications (ICACTA'22), SCOPUS, IEEE No: #54488 ISBN No

Xplore: 978-1-6654-9515-8, Coimbatore, India, 4-5 March 2022, DOI: 10.1109/ICACTA54488.2022.9753501

[55]. A.; Tripathi, C.M.; Perwej, Y.; Srivastava, A.K.; Kulshrestha, N. Face Recognition Based Automated Attendance Management System. Int. J. Sci. Res. Sci. Technol. 2022, 9, 261–268, 2022

[56]. Y. Lei, N. Scheffer, L. Ferrer and M. McLaren, "A novel scheme for speaker recognition using a phonetically-aware deep neural network", 2014 IEEE Inte. Conf. on Acoustics Speech and Signal Proc. (ICASSP), pp. 1695-1699, 2014

[57]. Yusuf Perwej, Firoj Parwej, "Perceptual Evolution of Playout Buffer Algorithm for Enhancing Perceived Quality of Voice Transmission over IP", International Journal of Mobile Network Communications & Telematics (IJMNCT), which is published by Academy & Industry Research Collaboration Center (AIRCC), USA, Volume 2, No. 2, Pages 1- 19, 2012 , DOI: 10.5121/ijmnct.2012.2201

[58]. Yusuf Perwej, Prof. (Dr.) Syed Qamar Abbas, Jai Pratap Dixit, Dr. Nikhat Akhtar, Anurag Kumar Jaiswal, "A Systematic Literature Review on the Cyber Security", International Journal of Scientific Research and Management (IJSRM), ISSN (e): 2321-3418, Volume 9, Issue 12, Pages 669 - 710, 2021, DOI: 10.18535/ijsrm/v9i12.ec04

[59]. A. Loutfi and S. Coradeschi, "Forming Odour Categories Using an Electronic Nose", Proc. European Conf. Artificial Intelligence (ECAI 04), pp. 119-124, 2004

[60]. A. Morales, M. Falanga, J. Fierrez, C. Sansone and J. Ortega-Garcia, "Keystroke dynamics recognition based on personal data: A comparative experimental evaluation implementing reproducible research", 2015 IEEE 7th International Conference on Biometrics Theory Applications and Systems (BTAS), pp. 1-6, 2015

[61]. Yau Wei Yun, "The '123' of Biometric Technology", Synthesis Journal, Pages 83-95, 2002

[62]. A. Dantcheva, P. Elia and A. Ross, "What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics", IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 441-467, Mar. 2016

[63]. Yusuf Perwej, "The Ambient Scrutinize of Scheduling Algorithms in Big Data Territory", International Journal of Advanced Research (IJAR), ISSN 2320-5407, Volume 6, Issue 3, Pages 241-258, 2018, DOI: 10.21474/IJAR01/6672

[64]. T. F. Cootes, C. J. Taylor, D. H. Cooper, and J. Graham, Active Shape Models their Training and Application. Comput. Vis. Image Underst., 1995

[65]. J. Matas, M. Hamouz, K. Jonsson, J. Kittler, Y. Li, C. Kotropoulos, A. Tefas, I. Pitas, T. Tan, H. Yan, F. Smeraldi, J. Begun, N. Capdevielle, W. Gerstner, S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz. Comparison of Face Verication Results on the XM2VTS Database. In Proc. 15th Int'l Conf. Pattern Recognition, volume 4, pages 858{863, Barcelona, 2000

[66]. D. Stewart, R. Seymour, A. Pass and J. Ming, "Robust audio-visual speech recognition under noisy audio-video conditions", IEEE Transactions on Cybernetics, vol. 44, no. 2, pp. 175-184, 2014

[67]. E. Şaykol, Web-based user interface for query specification in a video database system, M.S. thesis, Dept. of Computer Engg., Bilkent University, Ankara, Turkey, 2001.

[68]. E. Şaykol, U. Güdükbay and Ö. Ulusoy, A semi-automatic object extraction tool for querying in multimedia databases, MIS'01, Capri, Italy, pp. 11-20, 2001

[69]. Al-Mushayt O., Haq Kashiful, Yusuf Perwej, "Electronic-Government in Saudi Arabia; a Positive Revolution in the Peninsula", International Transactions in Applied Sciences, India, ISSN-0974-7273, Volume 1, Number 1, Pages 87-98, 2009

[70]. E. Bailly-Bailliere, S. Bengio, F. Bimbot, M. Hamouz, J. Kittler, J. Mariethoz, J. Matas, K. Messer, V. Popovici, F. Poree, B. Ruiz, and J.-P. Thiran, BThe BANCA database and evaluation protocol,[in Proc. Audio- and Video-Based Biometric Person Authentication, Guilford, pp. 625–638, 2003

[71]. D. Ciresan, "Multicolumn Deep Neural Networks for Image Classification", Proceedings of the 2012 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) CVPR '12, pp. 3642-3649, 2012

[72]. Aparna Trivedi, Chandan Mani Tripathi, Dr. Yusuf Perwej, Ashish Kumar Srivastava, Neha Kulshrestha, "Face Recognition Based Automated Attendance Management System" , International Journal of Scientific Research in Science and Technology(IJSRST), Volume 9, Issue 1, Pages 261-268, January 2022, DOI: 10.32628/IJSRST229147

[73]. Yusuf Perwej, "The Ambient Scrutinize of Scheduling Algorithms in Big Data Territory", International Journal of Advanced Research (IJAR), Volume 6, Issue 3, Pages 241-258, 2018, DOI: 10.21474/IJAR01/6672

[74]. Y. Zhang, D.-w. Gong and J. Cheng, "Multi-objective particle swarm optimization approach for cost-based feature selection in classification", IEEE/ACM Transactions on Computational Biology and Bioinformatics (TCBB), vol. 14, no. 1, pp. 64-75, 2017

[75]. Bhavya Singh Chauhan, Km Divya, Nikhat Akhtar, Vipin Rawat, Jitendra, "QR Code-based Real-Time Intelligent Attendance Covering System", International Journal of Computer Science Trends and Technology (IJCST), Volume 10, Issue 3, Pages 204-212, 2022, DOI: 10.33144/23478578/IJCST-V10I3P36

[76]. Perwej, Y., Abbas, S.Q., Dixit, J.P., Akhtar, N. and Jaiswal, A.K. , "A systematic literature review on the cyber security", International Journal of Scientific Research and Management (IJSRM), Vol. 9 No. 12, pp. 669-710,2021

[77]. M. Golfarelli, D. Maio, and D. Maltoni, "On the error-reject tradeoff in biometric verification systems," IEEE Trans. Pattern Anal. Machine Intell., vol. 19, pp. 786–796, July 1997

[78]. T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," Proc. SPIE, vol. 4677, pp. 275–289, Feb. 2002

[79]. E. d. Os, H. Jongebloed, A. Stijsiger, and L. Boves, "Speaker verification as a user-friendly access for the visually impaired," in Proc. Eur. Conf. Speech Technology, Budapest, Hungary, pp. 1263–1266, 1999

[80]. Y. Perwej, Nikhat Akhtar, Firoj Parwej, "A Technological Perspective of Blockchain Security", International Journal of Recent Scientific Research (IJRSR), Volume 9, Issue 11, (A), Pages 29472 – 29493, 2018, DOI: 10.24327/ijrsr.2018.0911.2869

Cite this article as :

Bhavesh Kumar Jaisawal, Dr. Yusuf Perwej, Sanjay Kumar Singh, Susheel Kumar, Jai Pratap Dixit, Niraj Kumar Singh, "An Empirical Investigation of Human Identity Verification Methods", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 1, pp. 16-38, January-February 2023. Available at doi : https://doi.org/10.32628/IJSRSET2310012

Journal URL : https://ijsrset.com/IJSRSET2310012