Publisher homepage: www.universepg.com, ISSN: 2663-7804 (Online) & 2663-7790 (Print)

https://doi.org/10.34104/ajeit.023.01410153

Australian Journal of Engineering and Innovative Technology

Journal homepage: www.universepg.com/journal/ajeit

Comparative Analysis of Different Biometric Techniques for Security Systems

Mohammad Saber Niazy[1]*, Nijad Ahmad[2], Zargay Habibi[2], Badam Niazi[3], and Nasrullah[4]

[1,2&4]Department of Computer Science, Khurasan University, Jalalabad, Nangarhar, Afghanistan; [2&3]Department of Computer Science, Nangarhar University, Afghanistan.

*Correspondence: niazi.edu@gmail.com (Mohammad Saber Niazy, Department of Computer Science, Khurasan University, Jalalabad, Nangarhar, Afghanistan).

ABSTRACT

Biometrics is the automated process of identifying a person based on biological and behavioral characteristics. It can be used to determine your identity and strengthen your ability to use accurate, secure, reliable, and less expensive authentication for a large number of applications. Biometry has been successfully implemented in numerous disciplines, including criminology, medicine, security, identity, and authorization. This article is all about Comparison Analysis of five biometric identification technologies i.e., iris recognition, fingerprint, voice recognition, face recognition, and signature recognition. It also discusses the mode of operation, and advantages And disadvantages of each above technology, application, limitation, acceptance, uniqueness, security, and performance. The author has concluded that the fingerprint technique is the fastest and most accurate biometric technique for a more dependable and secure system based on performance and fast communication. Due to the unique characteristics of the iris (the iris approach delivers the most secure performance, accuracy, uniqueness, and acceptability of all biometric procedures). It can be also used forever as a password. Finally, Iris is the only part of a human that cannot be changed and provides the finest answer overall.

Keywords: Biometrics, Applications, Physiological, Behavioral, Identification, and Techniques.

INTRODUCTION:

Biometric application development, such as facial recognition, has recently become a key priority for smart cities. In addition, researchers worldwide have worked hard on algorithms and approaches that will make these systems useful in everyday Life. Any security measures must ensure the safety of all sensitive information. Passwords are the most prevalent form of identification. As information technology and security algorithms advance, however, more and more systems are starting to rely on biometric variables for the recognition purposes (Ouerhani and Alfalou, 2010; Yan and Wang, 2018; Patel and Kale, 2018). These biometric features allow for individual identification based on some aspect of their physiology or behavior. They also offer many benefits. For instance, the necessity for many passwords or secret codes is eliminated if a person is simply ahead of the sensor. Several biometric recognition methods, including iris, fingerprint, voice, and facial recognition, have been implemented recently (Roy *et al*., 2023).

Measuring and interpreting biological data for authentication or identification is the ground of study known

as biometrics. Biometrics studies how an individual can be recognized through physical or behavioral traits. Biometric identification systems date back to ancient Egypt. We call "biometrics" the science of identifying individuals through collecting and analyzing information about their unique physical or behavioral characteristics. From the Ancient Greek (bios) for life and (metrics) for measurement comes our modern English word "biometric," which means "life measurement." The geometry of the face, fingerprints, D.N.A., ears, irises, retinas, and hands are all examples of physical traits. A person's behavior or dynamic measurements might be reflected in their Signature, voice, and gait, all of which are considered the behavioral traits (Jain and Ross, 2016; Jain and Prabhakar, 2004; Jain and Pankanti, 2006). Here is a growing concern for safety in today's world of sophisticated digital Technology, prompting the creation of various biometric-based personal authentication solutions. Using a person's distinctive behavioral or physical characteristics, biometrics provides a dependable and secure identification method. In personal identity systems, fingerprint recognition is the maximum widespread usage of biometrics. Furthermore, fingerprint authentication is one of the safest and most reliable biometric recognition methods. Because fingerprints are permanent and unique to each individual, they are the best candidate for biometric security systems (Jain and Ross, 2016). A distinctive pattern of interlaced valleys and ridges on the finger surface characterizes a fingerprint. A single curved segment represents a ridge, and a valley is a space between neighboring ridges. The two primary categories automated fingerprint recognition systems fall into are verification and identification. The benefits of biometrics are summarized in **Fig. 1**; **Fig. 2** lays out the benefits and drawbacks of biometrics (Kamlaskar and Abhyankar, 2021).

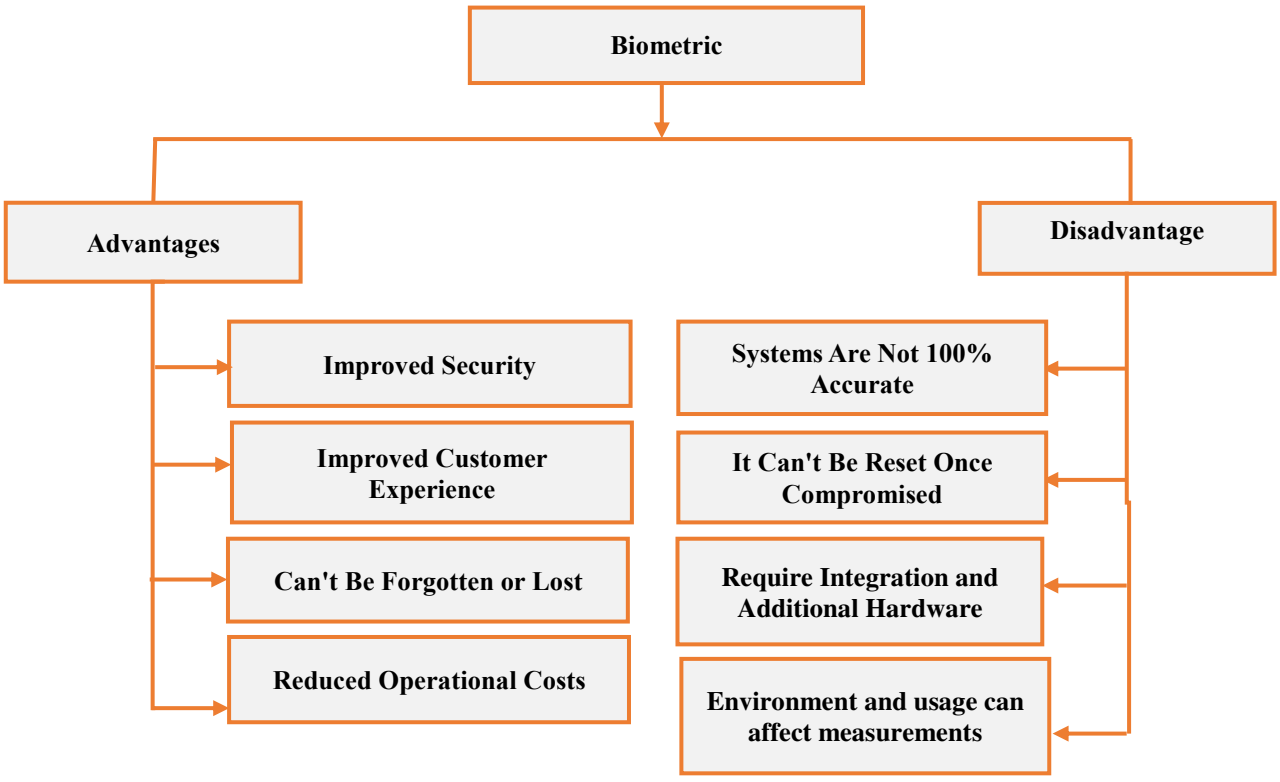

Fig. 1: Advantages and Disadvantages of Biometrics.

Pattern recognition techniques provide the basis of biometrics. Using biometrics in places like forensics, security, A.T.M.s, smart cards, personal computers, and even networks is becoming increasingly common. When compared to more traditional authentication techniques, biometrics offers more safety. This paper (Sabhanayagam & Senthamaraikannan, 2018) focuses on biometric recognition systems and provides a literature review of other methods of siding. Biometric recognition technologies circumvent the limits of

manual recognition systems. Yet, there are constraints on biometrically-based systems that can be addressed as biometric Technology develops. As can be shown in Table, biometrics is used in a wide variety of the contexts.

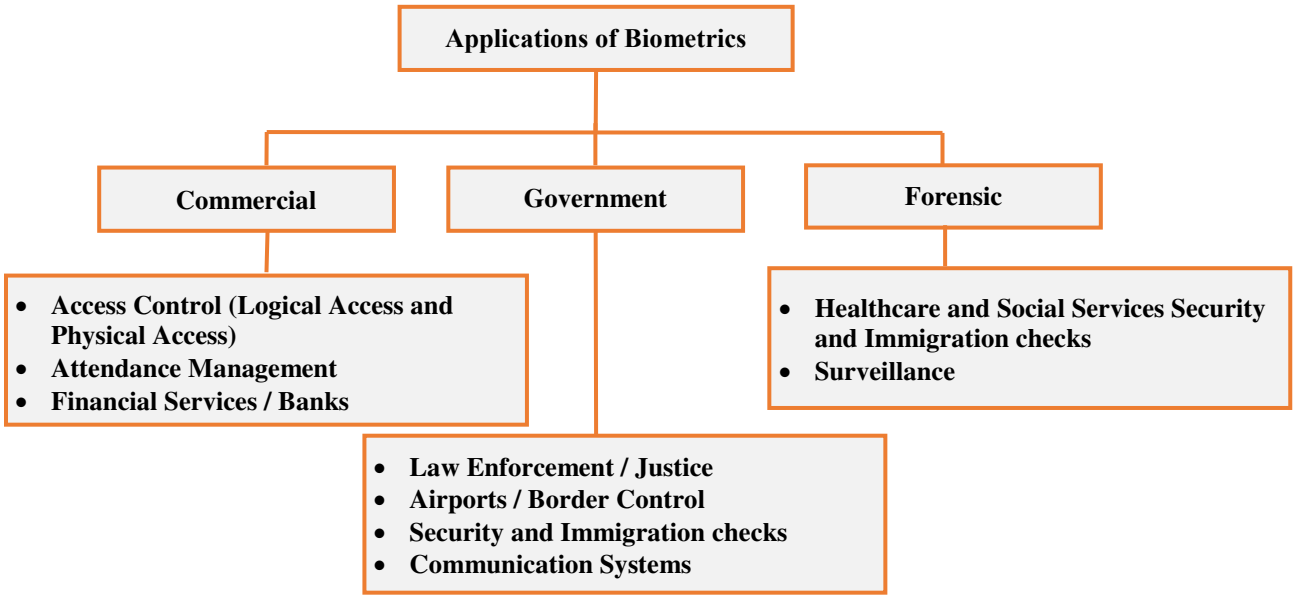

Fig. 2: Applications of Biometrics.

Automatic airport check-in, access systems, humanitarian aid operations, and many more can all benefit from iris recognition technology because it is one of the most reliable biometric technologies for human identification and verification. Rings, corona, crypts, contraction furrows, ciliary processes, freckles, and color are the rich textural information (Maltoni & Prabhakar, 2009) that may be extracted from an iris pattern. Iris designs are one-of-a-kind, easily recognizable, completely harmless, and remarkably consistent over time. The most distinguishing features of a person's iris pattern must be extracted for reliable iris recognition. Thus, it is essential to select an appropriate feature extraction approach (Sahu and Shrivas, 2013).

Characteristics of Biometric

It's important to remember that no biometric is perfect. It's not simple to draw parallels. The Researchers characterize the essential characteristic needs of any biometric qualities included in the table as the following: universality, uniqueness (distinctiveness) collectability, permanence, acceptability, performance, and resistance to circumvention (Sabhanayagam and Senthamaraikannan, 2018). These factors are often called the "seven pillars of biometrics" (Sarkar and Singh, 2020). **Fig. 3** provides a comparison of these features across popular biometric methods.

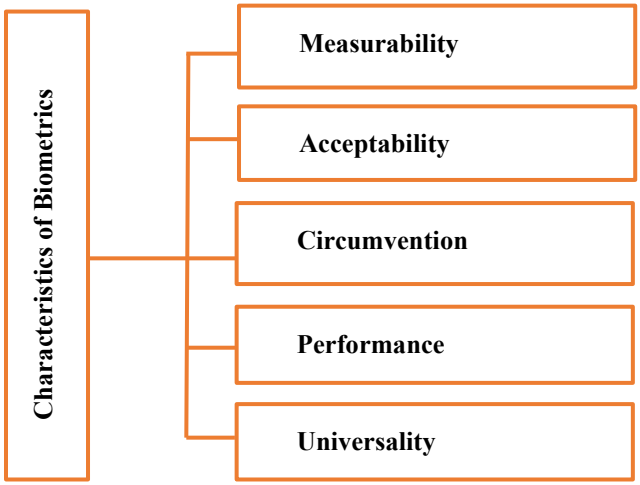

Fig. 3: Characteristics of Biometrics.

Individuals' fingerprints, irises, faces, hand veins, D.N.A., voices, signatures, gaits, typing patterns, and other biometric modalities can validate or authenticate them with a high grade of certainty. Traditional authentication systems rely on P.I.N.s, passwords, tokens, and the like, all of which can be compromised if hackers access them. Yet, biometric verification is quickly replacing more traditional forms of authen-

tication. Biometrics, which considers a person's unique physical and behavioral characteristics, offers the similar level of the security as other, more traditional authentication and verification methods (Bolle and Senior, 2013). Individuals can be dependably recognized by the biometric verification system using both observable and non-observable characteristics. Biometric identification uses physical identifiers, including a person's face, fingerprints, finger shape, iris, vein, retina, voice, and D.N.A., as the depicted in **Fig. 4**.

Fig. 4: Examples of Different Biometric Traits.

Five unique components comprise a biometric identity system: a sensor, feature extractor, template database, matcher, and decision maker. As shown in **Fig. 2**, a typical biometric authentication system may be created in (Wang and Brosseau, 2017).

Biometric System Modes

Fig. 5 depicts the two modes of process that the biometric authentication system can operate in enrollment and verification. There are two sub-steps in the authentication procedure: verification and identification. In addition, positive and negative identification are distinguished. These modes will be discussed at length in the following section (Jung and Heo, 2018).

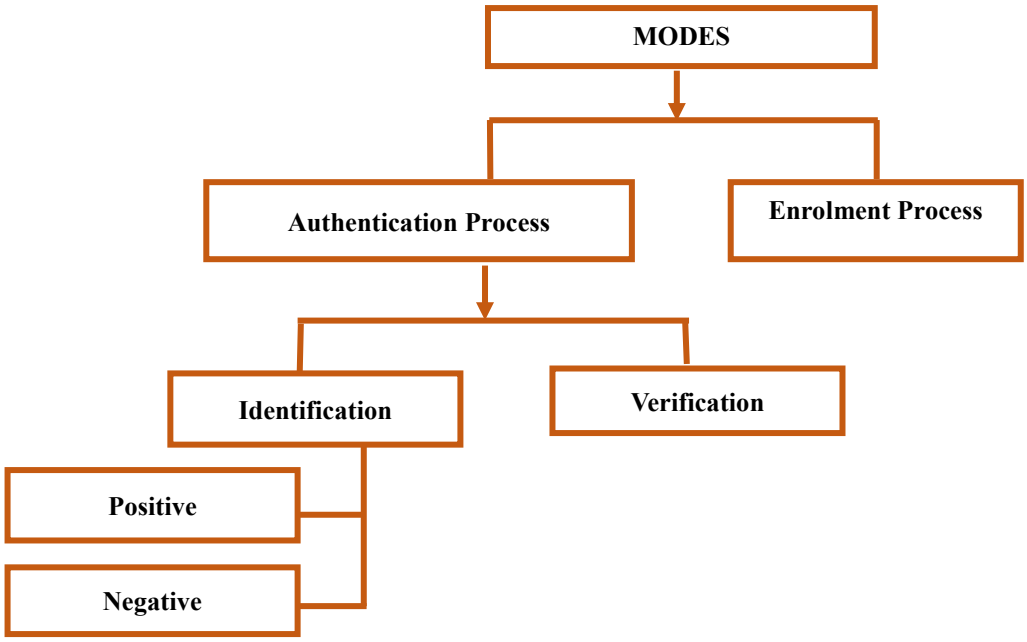

Fig. 5: Modes of Biometric system.

Using Biometric Methods

Biometrics is used to identify and verify individuals by measuring and comparing specific physical traits. Biometrics encompasses many methods that cannister be roughly broken down into two classes. Behavior and physiological traits are depicted in the **Fig. 6**. This study discusses fingerprint, iris, and facial biometrics on the physiological side and voice, Signature, and keystroke biometrics on the behavioral side (Jung and Heo, 2018).

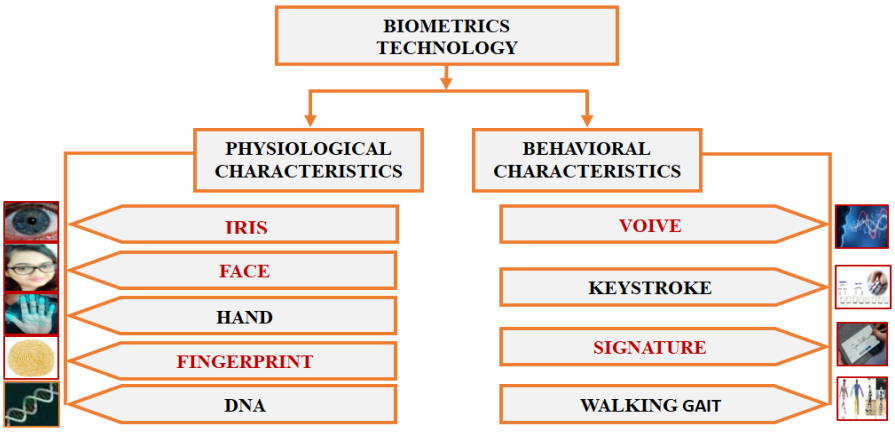

Fig. 6: Types of Biometric Techniques.

Types of Biometric Identifiers

Fingerprint Recognition

One of the greatest widespread and long-standing identification methods today is fingerprinting. Fingerprints are unique to each person because they feature a complex pattern of lines, arches, loops, and whorls. To implement this method, an ink or digital scan of a person's fingertips records information about their fingerprints. Records of fingerprints are processed or saved as an image so that the minutiae, including whorls, arches, and loops, can be compared with other fingerprint data. This method involves the user gently pressing his finger in contradiction of a small reader surface (optical or silicon) for less than 5 seconds during the verification process. The reader is only around 2 inches square. A computer called a reader receives information from the scanner, which subsequently transmits the data to a database for compareson. The US, along with other countries, including Canada and the United Kingdom, use a record of fingerprint procedures called Automatic Fingerprint Identification System (AFIS). Fingerprints are an individual's Signature. Despite its importance, dry skin, a poor environment, or an injury might render this procedure ineffective despite its great dependability, precision, and uniqueness. There is now a big database of comparative specimens, and the search for matching can be finalized quickly thanks to modern fingerprint procedures backed by computer and laser technologies.

Face Recognition

A digital video camera is used in this technique to examine the details of still photos of a person's face. It considers every aspect of a person's face, from the distances between their eyes and nose to the widths of their mouths and jaws. When an operator poses in front of the camera, these readings are compared to those already kept in the database. The achievement of this method has limited its usage to verification systems. The participant stands about two feet from the camera, with their back to it. When a being logs in, the scheme looks for their face and checks it against their claimed identity or a facial database. The Facial Recognition Technology Database (FERET)'s primary goal is to advance autonomous facial recognition capabilities that cannister be used for security purposes. Verification takes less than 5 seconds. However, the user may need to adjust his face slightly before it works. Although widely adopted, this inexpensive Technology can be deceived by identical twins and age-related facial changes.

Essential Elements of a Facial Recognition System

Fig. 7 the three main phases of engineering's automated face recognition problem, from left to right: (1)

approximate face detection and normalization; (2) feature extraction and correct face normalization; and (3) classification (verification or identification) (Chihaoui and Ben Amar, 2016).

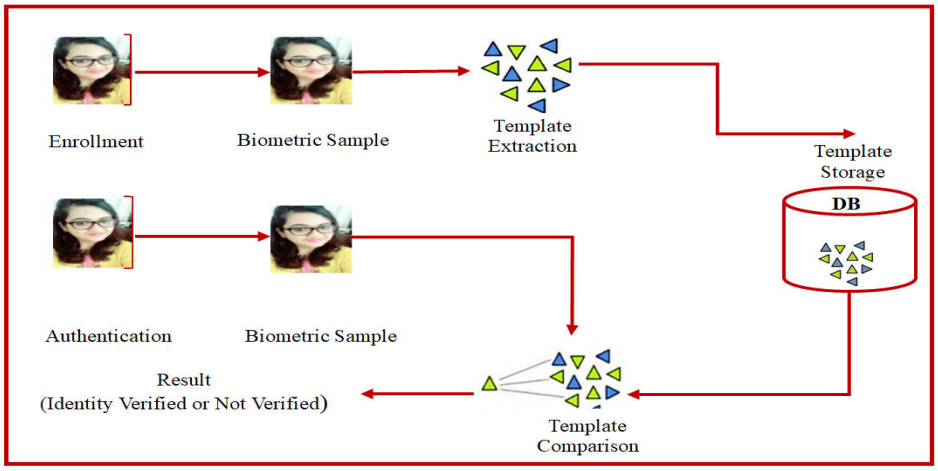

Fig. 7: The standard design of an automatic face-recognition system.

Iris recognition

Scannable features in the iris diaphragm, the pigmented tissue about the pupil, include over 200 data points. The user aligns him such that his reflected image appears on the screen. The iris scanner desires to be within 12-18 inches of the user, unlike the retinal scanner, which needs to be much closer. Since the user needs glance into the gadget, the Verification time is typically under 5 seconds. On the additional hand, this represents the user's actual iris pattern, either on a physical I.I.D. card or in a centralized database. The iris region of human eyes is captured in this photo database by a visible-light-operating sensor. If here is a correlation, the user is verified as legitimate. Iris scanning and recognition are quick and painless. When likened to fingerprints, it might be more FAR-effective. Iris recognition is more individual than fingerprinting but less so than retinal scanning. With almost 240 reference points for a match, this Technology is far superior to the fingerprint method, which only employs 60 points. Unlike fingerprinting, which requires physical contact, this method does not. They're better and safer than the alternatives, but they're also quite costly and require a high memory **Fig. 8** shows iris recognition Schemes.

Voice Recognition

Pitch, tone, frequency, and other nuances of the humanoid voice are analyzed and used by speech recognition software.

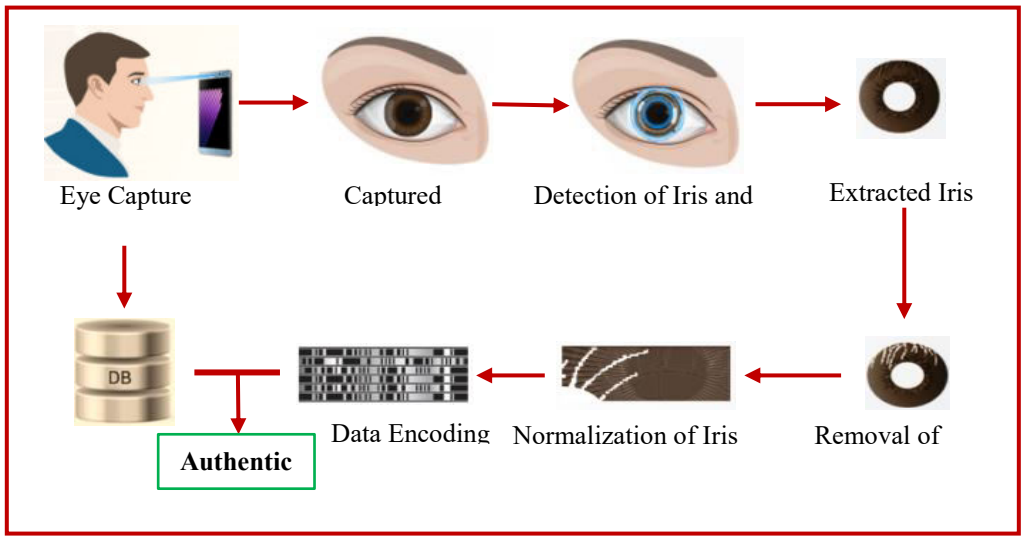

Fig. 8: Sample iris recognition Systems.

Different vocal tract shapes and acquired speech patterns are the primary emphases of this method. To use this method, the user speaks a command into a microphone connected to the device. Over twenty factors, including pitch, speech, energy density, wave-forms, etc., are used to investigate their voice and extract useful information. This real-time profile is compared to a previously recorded one in a central database. If here is a good match, the user is verified as legitimate. Although voice recognition is one of the easiest ways because it requires no training and costs very little to implement, it can be problematic in less-than-ideal conditions (such as when it's too cold or hot outside). When a person's voice changes, it's partly due to their appearance and habits. Male and female vocal cords vibrate at a rate of 80 and 400 times per second, respectively. Some characteristics that donate to the uniqueness of each person's voice are the scope of their jaw opening, the shape and position of their tongue, and their lips.

Signature Recognition

Signature recognition was the least reliable biometric method. In a signature, the text used is continuous and uniform. A tablet or paper is placed over a sensor tablet, and the user signs there. The verification process takes roughly 5 seconds while the device stores the user's Signature and comparisons it to its database. The technologies are promoted through a cheap writing tablet, which greatly increases the biometrics' cost-effectiveness without considerably reducing its performance accuracy. This Technology has minimal uniqueness despite being inexpensive, non-intrusive, widely accepted by users, requiring little training, and evolving.

Functioning of a Biometric System

This system's two modes of operation training and classification are both straightforward. Today's activeties are commonly observed, such as the operation of a fingerprint sensor on any cellular telephone. The saved fingerprint pattern is verified every time a finger touches the sensor. The diagrammatic depiction of this mechanism in action is provided below in **Fig. 9**. In this context, "enrollment" describes the primary step. The data is saved permanently within the system. After implementation, all of the information in the system is double - checked against what was gathered during enrollment to ensure accuracy.

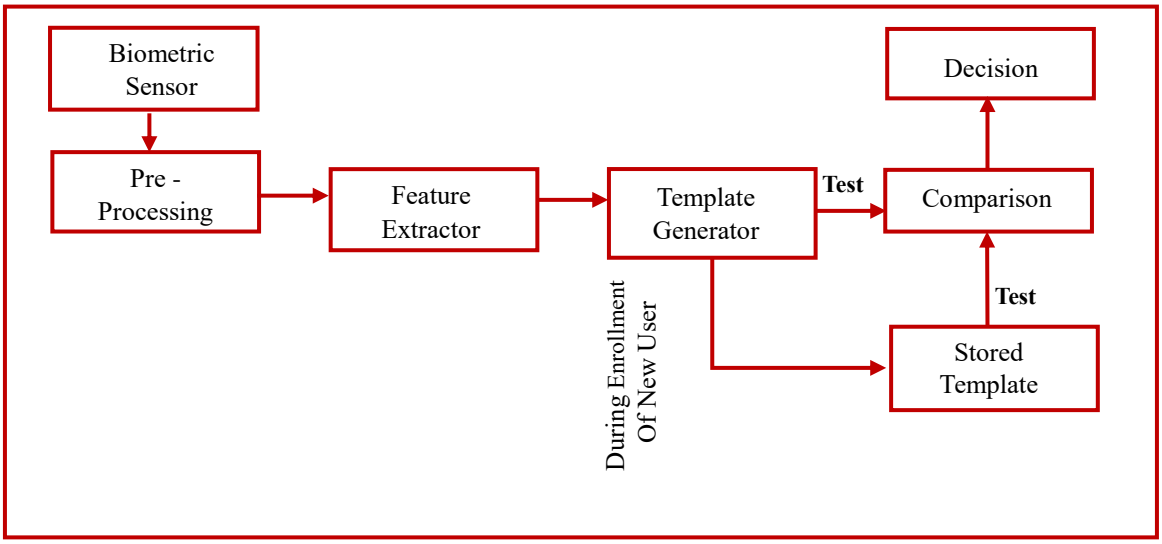

Fig. 9: Functioning of a Biometric System.

We need to make sure that the data is entered and stored safely. In the initial Building Block, the sensor acts as a user interface, gathering information from the outside environment. It's mostly a representation, but that might shift dependent on the system's use. The data from the sensor is modified and de-barred from further processing in the second Block. Important and necessary features are extracted in the following Feature Extractor Block. At this stage, retrieving the right features as efficiently as possible is crucial. The following Block, Template generator, uses the pictured integers with specific attributes to generate templates.

All relevant structures from the source have been rolled into this single template. Biometric measurements are segregated in templates to reduce file size and maintain individuality. Now that the template has been created, it may be protected in a database, matched with others, and sent to a human who will compare it to the currently active template and determine the degree of deviation using the algorithm. The generated data is output by the matching program after it has accessed the template (Sachdeva, 2021).

Advantages and Disadvantages of the Biometric Techniques

Many modern security systems make usage of Biometry identification methods. There are benefits and drawbacks to all of these methods. Based on the nature of the task at hand, the appropriate application and method can be chosen from **Table 1**.

Table 1: Advantages, Disadvantages and Applications of Biometrics methods.

Moods	Advantages	Disadvantages	Applications
Iris	▪ Only 1 in 10 people have an iris pattern that is a perfect match. ▪ Even fraternal twins have slightly distinct irises. ▪ Highly scalable ▪ Wearing glasses or contacts has no effect on accuracy. ▪ You won't be able to touch the system in any way. ▪ Promising processing time of 2 to 5 seconds due to small template size. ▪ Reduced probability of incorrect acceptance ▪ Constant over the course of a person's life ▪ Secure and unpredictable to a significant degree. ▪ The processes of encoding and making choices are manageable.	▪ Scanners can be fooled by high-quality photos. ▪ User input is required for reliable scanning. ▪ Because the user must remain still during the scanning process, usability is diminished. ▪ Less opposition in the market ▪ Eyelashes, lenses, and reflections make it impossible to see. ▪ Extremely long-distance challenges ▪ At risk of having subpar images	▪ Measuring can be impacted by context and usage. ▪ Migration and border control ▪ Public safety ▪ Healthcare Services ▪ Finance and banking
Fingerprint	▪ Advanced, State-of-the-Art Equipment. ▪ Comparatively inexpensive ▪ Further secure and highly reliable. ▪ Since the template size is modest, matching can take place quickly. ▪ Eats less memory space. ▪ Maximum widely used Technology ▪ High accuracy ▪ Ability to enroll multiple fingers ▪ Numerous possible settings for deployment ▪ Not disruptive, and not subject to organic evolution	▪ Barriers to identification may result from injuries such as cuts or scars, or from the loss of a digit. ▪ They can be readily fooled by wax replicas of fingers. ▪ Comes into actual contact with the machine. ▪ Uses a lot of computer processing power ▪ Deteriorated or subject to change throughout time ▪ Vulnerable to deterioration and distortion from dirt and kinks ▪ Some people have lost or ruined their fingerprints.	▪ Authentication of Driver's License ▪ Border Control/Visa Issuance. ▪ Access control in organizations. ▪ Law Enforcement Forensics
Face	▪ Non-intrusive, i.e., involves no physical contact	▪ Facial characteristics shift and shift as we age.	▪ Identity Verification.

	▪ Storing templates in a database is easy. ▪ Socially accepted ▪ It reduced statistical complexities for recognizing face images. ▪ Similar to the human process of authentication ▪ Convenience and Matured Technology ▪ The existing image-capturing devices, i.e., cameras, can be used. ▪ Faster the identification process	▪ Distinction is not a given when dealing with twins. ▪ Different facial expressions might have an impact on recognition accuracy. ▪ Extremely reliant on proper illumination for accurate input ▪ Because of privacy invasion, most people feel uneasy. ▪ Better suited for authentication purposes ▪ The data available in 2D is sparse. ▪ Unstable in response to changes in light, direction, or expression ▪ A mask or other form of facial concealment will render it ineffective.	▪ Access Control Verification. ▪ Human-Computer Interaction. ▪ Criminal Identification. ▪ Surveillance
Signature	▪ Forgery research has been considerable in the artificial Biometry system that is a signature. ▪ Inexpensive technology ▪ The signup process is simple and quick. ▪ Non-intrusive. ▪ It takes less space and responds quickly for signature verification in general. ▪ There is no need for the user to know how to write in English for the signature verification method to work. ▪ Little time for verification.	▪ There is a lot of history behind utilizing Signature for document authentication, but not security purposes. ▪ It isn't easy to use. ▪ It is a large template. ▪ To attain the required precision, the scheme may require a five-dimensional pen. This results in pricey hardware. ▪ Seeing how it's possible that not everyone can sign. ▪ Some persons have tremors or other motor control issues, and others simply lack the motor skills necessary for consistent handwriting. ▪ Signatures written by hand change throughout time.	▪ Banking. ▪ Passport verification system. ▪ Provides authentication to a candidate in the public examination from their signatures.
Voice	▪ Efficient, simple, and reliable. ▪ It allows you to write more quickly on a computer, tablet, or smartphone without having to type. ▪ Many industries, including the healthcare sector, can benefit from its increased productivity. ▪ It's significantly quicker at capturing speech than typing. ▪ You can use text-to-speech in real-time. ▪ The software has the similar spelling capabilities as a pen or a keyboard. ▪ Aids the hearing- and visually-impaired	▪ Some worry that privacy may be compromised because of the capability to record voice data. ▪ The program may have difficulty with the language, especially if there are technical terms involved. ▪ If you don't communicate clearly, it may misunderstand what you mean.	▪ Voice-Recognition Technology for Use in Translation Programs ▪ Voiceprint Technology for Use in Crime Scene Investigation and Forensics ▪ Voice Identification for Security ▪ Artificial Intelligence Helpers That Learn Your Voice ▪ Mobile Voice Recognized Payments

Review of Literature

In this part, the author discusses various previously published research papers on biometric systems:

In the present work (Sudar and Nagaraj, 2019). We have evaluated the utility of biometric procedures to more conventional authentication methods. Fingerprint, iris, retina, face, palm, voice, Signature, and gait biometrics are fair a few of the broad biometric methods we've covered, along with their benefits and downsides. General biometric approaches for security systems are compared and analyzed in this study. This study (Sabhanayagam and Senthamaraikannan, 2018) summarizes the various biometric approaches, discussing their benefits and drawbacks. The fingerprint is a fast and accurate biometric approach for a more dependable and secure system, according to a literature review that noted the differences and implications of error rates across other biometric techniques. The natural properties of the iris biometric modality lend credibility and non-intrusiveness to the iris identification system. Current efforts in this field pose difficulties for both small template sizes and quick verification techniques. The act of the iris recognition system has been optimized by making special efforts to decrease the size of the retrieved characteristics. We present a feature fusion method based on multilinear subspace learning to better examine Iris recognition. This strategy has four distinct phases. In the first stage, the iris is segmented out of the eye's visual image. As wavelet packet decomposition may provide good time and frequency resolutions concurrently, it is used in another stage to excerpt features of the iris image. After the nodes or packets have been separated, they are organized into a third-order tensor rather than a lengthy vector, and multilinear principal component analysis (MPCA) is then used to implement feature fusion (Kamlaskar and Abhyankar, 2021) directly. Extraction of tensor features using MPCA has found widespread use in many different computer image and design recognition tasks. Recognizing faces (Vasilescu and Terzopoulos, 2003), processing signals (Plataniotis and Venetsanopoulos, 2011), reading handwriting (Wang and Wang, 2016), recognizing digital numbers (Haiping and Plataniotis, 2008) analyzing content (Muhsain, 2011) and finding outliers in data (Jing, 2019) are all relatively new uses. The authors offer a new MPCA framework for dimensionality reduction and feature extraction of the tensor object and use it as an example in gait identification. Inspired by MPCA's effectiveness in feature extraction, we propose tensor-based MPCA feature fusion for Iris recognition. While the input samples of the back-propagation approach are coded and normalized using an algorithm working using a predefined codebook, N.F. (Muhsain, 2011) explored the challenge of minimizing the fingerprint features given into the neural network. The main benefits of making a codebook are its ease of use and quick processing time. Pre-processing for image enhancement, binarization and thinning of fingerprint images, feature extraction from the thinned image ridge, and finally a matching stage in which similarity and distance measurements are used to match two-minute points are all part of (Jing, 2019) 's proposed multi-stage fingerprint recognition system. In (Bakheet and Youssef, 2022) the use of ridge termination and ridge bifurcation as minutiae in fingerprint recognition using artificial neural networks (ANNs) is proposed. Safely extracting the details from the binary fingerprint images is the most important stage in automatic fingerprint matching. The presented method improves recognition rates while reducing mistake rates. The experimental findings demonstrated a recognition rate of 91.10 percent on the average using the planned technique. In (Bakheet and Youssef, 2022) ridge termination and ridge bifurcation are used as distinguishing features in an ANN-based fingerprint recognition algorithm. The most crucial part of automatic fingerprint matching is obtaining the details from the binary fingerprint images in a secure manner. The presented method improves recognition rates while reducing mistake rates. (Gronkiewicz and Mickiewicz, 2016) work is among the most reliable approaches for iris recognition. Iris structures are extracted using quadrature 2D Gabor wavelets, and the resultant image is encoded into a 256-byte (2048-bit) binary code. The degree to which two iris codes are similar is measured using the Hamming distance. A Laplacian of Gaussian filter is used in the Iris recognition system proposed in (Wildes, 2021). Finally, I built a Laplacian pyramid to make a small iris pattern. A way to describe an iris recognition system and explaining how to classify data employing a specific strategy was proposed by (Kaur,

2014). Iris recognition on demand is utilized in the academic world to ensure authenticity. The iris recognition system's inner workings must be spelled out in this study, but the corresponding approaches still have a way to go before they're truly robust. Many biometric functions were described by using a single parameter, as shown by the work of (Kaur and Verma, 2014). The first step in using a biometric function is extracting the consistent feature. A separate can be identified using the bio-metric system's parameters. Design recognition is the basis of biometrics. The military, forensics, controls, access, and other fields all use on-demand Biometric Technology. Dependent on the context, iris recognition can be an effective biometrics method. In (Saini and Rana, 2014) compare various biometric system methods. This article has to be defined as a quick introduction to various methodologies, which has to be utilized in an earlier paper and define the comparison by testing the performance on various types of databases and then classifying by various parameters. It has also specified the recognition techniques. Although biometrics security systems have various concerns like data privacy, bodily privacy, spiritual conflicts etc., they nonetheless have benefits that may improve our life magnificently by boosting security.

Simulation Resulting Table

Table 2: Comparative Analysis of Various Biometric Techniques.

Moods	Acceptance	Accuracy	Uniqueness	Performance	Security	Cost	FAR	FRR
Iris Scan	Medium	High	High	High	High	High	>=.001%	In 100 (2-10%)
Fingerprint	Medium	High	High	High	Medium	Medium	1 to 10 in 100,00 (.001-.01%)	3 to 7 in 100 (3-7%)
Face	Medium	Medium	Low	Low	Low	Medium	100 to 1000 in 100,000(.1-1%)	10 to 20 in 100 (10-20%)
Voice	High	Medium	Low	Low	Low	Medium	2000 to 5000 in 100,000 (2-5%)	10 to 20 in 100 (10-20%)
Signature	Very High	Low	Low	Low	Low	Medium	2-5%	10 to 20 in 100 (10-20%)

Several biometric methods are compared above for their precision, false acceptance and rejection rates, uniqueness, performance, acceptability, security, etc.

CONCLUSION:

In general, biometrics is based on pattern recognition techniques; moreover, it is an emerging technology widely used in security, forensics, smart cards, networks, personal computers, and A.T.M.s. Biometric verification is more secure than conventional authentication methods, besides several biometric approaches are analyzed and contrasted in this research, such as security, performance, precision, uniqueness, acceptability cost, acceptance rate, rejection rate, and many more which are already mentioned in above table widely. In light of the methodologies above and the comparison table, the author has concluded that the fingerprint technique is the fastest and most accurate biometric technique for more dependable and secure system based on performance and fast communication. Whereas, speech, face, and signature biometric techniques were mostly accepted by users. Due to the unique characteristics of the iris (the iris approach delivers the most secure performance, accuracy, uniqueness, and acceptability of all biometric procedures). It can be also used forever as a password. Finally, Iris is the only part of a human that cannot be changed and provides the finest answer overall.

ACKNOWLEDGEMENT:

The author(s) would like to thanks the participants and the members of researchers' families who provided support and assistance.

CONFLICTS OF INTEREST:

The author(s) confirm that this study has no potential conflict.

REFERENCES:

1) Bakheet, S., Al-Hamadi, A., & Youssef, R. (2022). A fingerprint-based verification framework using Harris and SURF feature detection algorithms. *Applied Sciences*, **12**(4), 2028. https://www.mdpi.com/2076-3417/12/4/2028
2) Bolle, R. M., Connell, J. H., & Senior, A. W. (2013). Guide to biometrics. *Springer Science & Business Media*.
3) Chihaoui, M., Bellil, W., & Ben Amar, C. (2016). A survey of 2D faces recognition techniques. *Computers*, **5**(4), 21. https://doi.org/10.3390/computers5040021
4) Gronkiewicz, M., Czajka, A., & Mickiewicz, P. (2016). Post-mortem human iris recognition. In 2016 International Conference on Biometrics (ICB) (pp. 1-6). *IEEE*.
5) Haiping, L., & Plataniotis Konstantinos, N. (2008). Venetsanopoulos Anasta-sios N, ". MPCA: Multilinear principal component analysis of tensor objects," Neural Networks, *IEEE Transactions on*, **19**(1), 18-39.
6) He, Y., Li, X., & Jing, X. (2019). A multiscale residual attention network for multitask learning of human activity using radar micro-Doppler signatures. *Remote Sensing*, **11**(21), 2584. https://doi.org/10.3390/rs11212584
7) Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern recognition letters*, **79**, 80-105.
8) Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, **14**(1), 4-20.
9) Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. *IEEE transactions on information forensics and security*, **1**(2), 125-143.
10) Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern recognition letters*, **79**, 80-105. https://doi.org/10.1016/j.patrec.2015.12.013
11) Jung, H. Y., & Heo, Y. S. (2018). Fingerprint liveness map construction using convolutional neural network. *Electronics Letters*, **54**(9), 564-566.
12) Kamlaskar, C., & Abhyankar, A. (2021). Multilinear principal component analysis for iris biometric system. *Indonesian J. of Electrical Engineering and Computer Science*, **23**(3), 1458-1469.
13) Kaur, G., & Verma, C. K. (2014). Comparative analysis of biometric modalities. *Inter J. of Advanced Research in Computer Science and Software Engineering*, **4**(4), 603-613. https://paperzz.com/doc/8129867/comparative-analysis-of-biometric-modalities
14) Kaur, N., & Juneja, M. (2014). A review on iris recognition. 2014 Recent Advances in Engineering and Computational Sciences (*RAECS*), 1-5.
15) Lu, H., Plataniotis, K. N., & Venetsanopoulos, A. N. (2011). A survey of multilinear subspace learning for tensor data. *Pattern Recognition*, **44**(7), 1540-1551. https://doi.org/10.1016/j.patcog.2011.01.004
16) Maltoni, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition (Vol. **2**). *London: springer*.
17) Muhsain, N. F. (2011). Fingerprint Recognition using Prepared Codebook and Back-propagation. Al-*Mansour J.,* **15**(1), 31-45.
18) Ouerhani, Y., Jridi, M., & Alfalou, A. (2010). Fast face recognition approach using a graphical processing unit "GPU". In 2010 IEEE International Conference on Imaging Systems and Techniques (pp. 80-84). *IEEE*. https://ieeexplore.ieee.org/abstract/document/5548545
19) Patel, N. P., & Kale, A. (2018). Optimize approach to voice recognition using iot. In 2018 International Conference on Advances in Communication and Computing Technology (ICACCT) (pp. 251-256). *IEEE*.
20) Roy S, Kabir MH, and Ahmed MT. (2023). IoT based low-cost smart home automation and security system using wireless technology. *Aust. J. Eng. Innov. Technol*., **5**(3), 101-112. https://doi.org/10.34104/ajeit.023.01010112
21) Sabhanayagam, T., Venkatesan, V. P., & Senthamaraikannan, K. (2018). A compre-

hensive survey on various biometric systems. *Inter J. of Applied Engineering Research*, **13**(5), 2276-2297.

22) Sachdeva, K. (2021). A Review Paper for Security by Using Biometric Fusion.
23) Sahu, D., & Shrivas, R. (2013). Fingerprint reorganization using minutiae-based matching for identification and verification. *Inter J. of Science and Research*. https://paper.researchbib.com/view/paper/320754
24) Saini, R., & Rana, N. (2014). Comparison of various biometric methods. *Inter J. of Advances in Science and Technology*, **2**(1), 24-30.
25) Sarkar, A., & Singh, B. K. (2020). A review on performance, security and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications*, **79**, 27721-27776.
26) Sudar, K. M., Deepalakshmi, P., & Nagaraj, P. (2019). Analysis of security threats and counter measures for various biometric techniques. In 2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES) (pp. 1-6). *IEEE*.
27) Vasilescu, M. A. O., & Terzopoulos, D. (2003). Multilinear subspace analysis of image ensembles. In 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2003. Proceedings. (Vol. **2**, pp. II-93). *IEEE*. https://link.springer.com/chapter/10.1007/0-387-27257-7_8
28) Wang, Q., Alfalou, A., & Brosseau, C. (2017). New perspectives in face correlation research: a tutorial. *Advances in Optics and Photonics*, **9**(1), 1-78.
29) Wang, Q., Kang, W., & Wang, Y. J. (2016). Support Tensor Machine Image Classification Algorithm Based on Tensor Principal Component Analysis. *J. Inf. Hiding Multim. Signal Process.,* **7**(6), 1265-1273.
30) Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2018). A fingerprint and finger-vein based cancelable multi-biometric system. *Pattern Recognition*, **78**, 242-251. https://doi.org/10.1016/j.patcog.2018.01.026

Citation: Niazy MS, Ahmad N, Habibi Z, Niazi B, and Nasrullah, (2023). Comparative analysis of different biometric techniques for security systems. *Aust. J. Eng. Innov. Technol.*, **5**(3), 141-153. https://doi.org/10.34104/ajeit.023.01410153