ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAR886

Analysis of Biometric Authentication Techniques: A Review

Vivek kumar[1]; K Nageshwara Rao[2]
[1,2]Defence Scientific Information and Documentation Centre, DRDO

Abstract:- This report delves into diverse biometric authentication techniques and offers an overview of their evolution, applications, limitations, advancements, and comparative attributes. It also highlights biometric authentication's pivotal role in elevating security and convenience across sectors.

Keywords:- *Biometrics, Verification, Authentication, Liveness Detection, Multimodal Biometrics.*

I. INTRODUCTION

The word Biometry is derived from two Greek words: “Bio” meaning life, and “metric” meaning measurement. Biometric authentication is a security mechanism that analyses and compares a person's unique physical or behavioral traits during the enrolment phase. The ability of biometrics to validate rapidly and effectively returning clients is its most significant advantage. Biometric data provides a secure alternative to pin codes, passwords, and knowledge-based authentication because it is unique to everyone. During the enrolment process, the system collects biometric data and develops a unique template for the person. To confirm the individual's identity, the system compares the given biometric data with the saved template during subsequent identification attempts. Because it is difficult to fabricate or copy these unique traits, biometric identification is regarded more secure and convenient.

II. TYPES OF BIOMETRICS

There are two different types of biometric techniques- Physiological and Behavioral. This review focuses on commonly used physiological biometrics. With rapid development in this field of technology, different techniques for authentication have been developed which provide multiple features for different applications as per the requirements. Some of these techniques include:

- *Fingerprints*
- *Vein Recognition*
- *Iris Recognition*
- *Retina Scanning*
- *Facial Recognition*
- *Hand Geometry*

Behavioral biometrics include Voice recognition, Gait recognition, keystroke dynamics etc. [2]

These techniques can be categorized in different ways such as time required for identification, physical contact, accuracy, security, and the system’s ability to adapt to change. [22]

III. APPLICATIONS

➤ *Biometric Technology is Becoming more Common, and hence its Applications are Expanding. Here are some Typical Examples:*

- Immigration and border control: Arriving and departing individuals are subjected to biometric screening at the US border. It enables CBP agents to detect national security dangers as well as visa overstays.
- The execution of the law; Biometrics are commonly used by police personnel to aid in criminal investigations. Biometric face identifiers, for example, are particularly useful for locating people on watchlists and verifying identities in instances where a person cannot identify themselves.
- Airport safety: Biometrics have been used to verify passenger identity at many major airports. It contributes to a faster self-check-in process and a better passenger boarding experience.
- Authentication and access to mobile devices: When electronic identification is required, biometric technology provides an additional layer of protection.
- Banking: Client identification and authentication solutions that are strong and secure are required by anti-money laundering and Know Your Customer rules. Banks can avoid fraud, such as identity theft and spoofing, by employing biometric security.
- The Internet of Things (IoT): Many smart devices make use of biometrics. Home assistants, for example, use voice as a biometric identifier.

The application of biometric authentication identification holds immense potential to revolutionize security measures, enhance user convenience, and ensure a more reliable and efficient means of verifying identity in various sectors while necessitating careful consideration of privacy, security, and ethical implications for its widespread adoption.

IV. DEVELOPMENT

In the rapidly evolving landscape of technological advancements, few domains have witnessed as remarkable a transformation as the field of biometrics. Over the past few decades, the fusion of computer science, data analytics, and physiological sciences has led to extraordinary strides in identifying, verifying, and authenticating individuals through their unique biological characteristics. From its developing origins of fingerprint recognition to the contemporary frontiers of facial recognition, iris scanning, and voice analysis, the field of biometrics has not only revolutionized personal security but has also found applications in diverse sectors as mentioned above.

A. Fingerprint Recognition

The presence of special raised lines on the skin creates unique fingerprints. Humans have these lines on their fingers, thumbs, palms, toes, and foot soles. These lines help provide friction and give us more grip with objects in contact with human skin. These ridges make patterns which have gaps and breaks in them. These breaks are called "minutiae." These unique breaks are random and can be used to identify users apart because no two pieces of skin with these lines have the same pattern of breaks. Due to the uniqueness of the fingerprints, they can be used to identify individuals.

➢ *History and Evolution:*

Archaeological evidence in China proves that fingerprints have been used dating back to at least 7000 to 6000 BC. Earthenware marked with fingerprints (speculated to be marked as a signature of the potter, although the evidence is insufficient) have been found in archaeological sites in China and ancient Assyria.

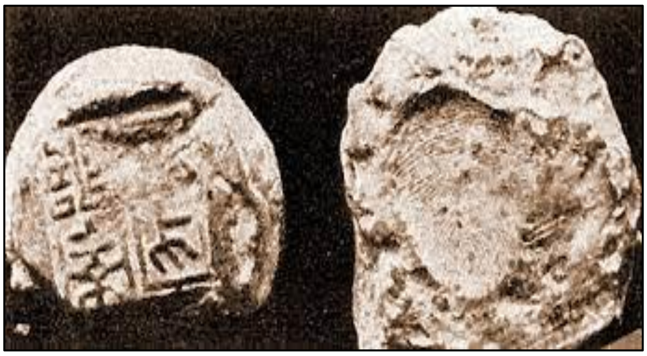

Fig 1 Fingerprints Found in Archaeological Sites in China [A. Sutherland Ancient Pages.com]

In mid-1800's, studies began to establish the uniqueness of each fingerprint to an individual and no two prints can have the exact same ridge patterns and minutiae. Fingerprint identification was picked up by Argentina for criminal identification in 1896, then at Scotland Yard in 1901 and many other countries in early 1900's.

1980s brought huge innovations in personal computers and optical scanners that provided fast processing of the images hence enabling fingerprint identification technology to grow in more domains. Development of inexpensive scanners in 1990s boosted growth for the 21st century. [5]

➢ *Limitations:*

- Noisy Data: External factors like dust or dirt can interfere with fingerprint scans, potentially leading to inaccurate results as the scanner may pick up these contaminants along with the fingerprint pattern.
- Wear and Tear: Over time, the condition of a person's fingertips can change due to natural wear and tear, which may alter the fingerprint's characteristics. Additionally, wet or moist fingertips can affect the quality of the fingerprint image, impacting recognition accuracy.
- Reduced Sensitivity: The level of contact between the fingerprint scanner and the finger can impact sensitivity and reliability. Insufficient contact may lead to incomplete scans, affecting the system's ability to recognize the fingerprint accurately. [13]

➢ *Advancements:*

- *Infrared Laser Ablation Technology at Crime Scenes*

Initially a photo of the fingerprint was captured, and a cotton swab sample taken to a laboratory to identify the chemical compounds. This method was not very accurate. Use of laser ablation has allowed more efficiency and further optimized the results to be more precise.

Infrared Laser Ablation technology involves the use of lasers to scan the acquired quiescent prints. These prints are then heated to accumulate high energy in one small region. When the chemical bonds reach threshold heat, they start to stretch and eventually explode, which ends up lifting them off the surface for further examination. This technology can be employed to analyze fingerprints, genetic materials, lipids, proteins and even explosives. Laser ablation has allowed huge amounts of development in the field of crime investigations and forensics. [5]

- *Multimodal Approach*

Multiple biometric technologies can be infused to improve the reliability of the system and ensure more security. One such example is multimodal fingerprint and finger vein recognition. The proposed combination of modalities increases the recognition rate and the FAR and FRR for this system are 0.23 and 0.1 respectively. [18]

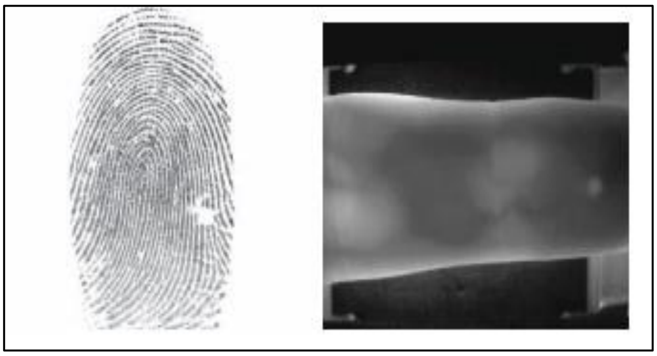

Fig 2 Fingerprint and Finger Vein Geometry of a Finger [18]

➢ *State-of-the-Art*

Fingerprint recognition employs a range of methods to accurately identify individuals based on their unique fingerprint patterns. These methods encompass diverse techniques, including ridge-based analysis, minutiae extraction, and directional image processing. Each approach plays a pivotal role in extracting distinctive features and patterns from fingerprints, contributing to the effectiveness and reliability of fingerprint recognition systems.

- *Directional Image*

A directional image is like a pixelated map that shows the general directions of the ridges in a fingerprint. This type of image helps capture the main fingerprint pattern and works well even when the fingerprint is unclear due to noise. It can also help fix the ridge directions in parts of the fingerprint that might be damaged. This is done through a process called regularization. These directional images are quite popular in the methods used to categorize fingerprints. [53, 54]

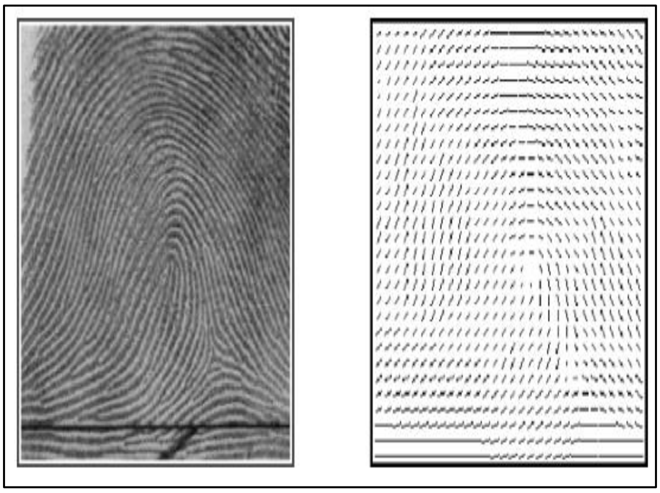

Fig 3 A Fingerprint Image and the Corresponding Directional Image in a 32x32 Grid Format [53, 54]

- *Singular Points*

The lines on a fingerprint typically run alongside each other, however they can occasionally create distinctive spots known as the core and delta. When at least one ridge enters from the side, loops back, and then continues on the same side, a core forms. Ridges enter and meet the curved ones on the other side of the core. Some ridges run above the core, while others flow under it. The delta is defined as the intersection of these divergent ridges closest to the core. [17]

Figuring out these special points in a fingerprint isn't easy, especially if the fingerprint image isn't clear. But knowing where these points are can be helpful. They're used to position fingerprints correctly and to classify them. Usually, this is done using a directional image rather than the original image, which helps capture the ridge directions [50, 52]. These special points can provide essential landmarks for aligning fingerprints and aiding in their classification.

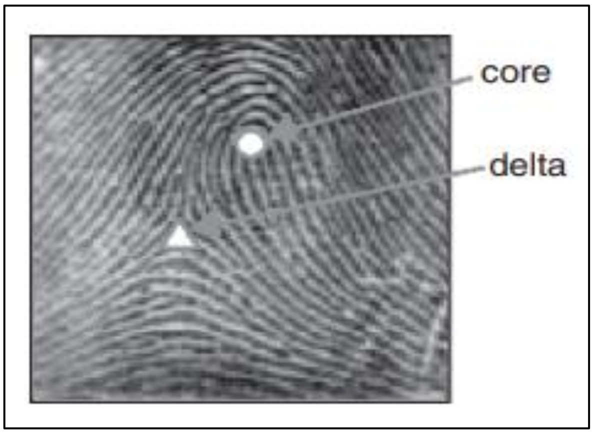

Fig 4 Core and Delta Points in a Fingerprint Image [17]

- *Ridgeline Flow*

The direction of the ridges is a key identifying characteristic. Although it can be challenging to accurately find it in unclear fingerprints, it's more reliable than individual points. Ridges are often obtained directly from the directional image, or by converting the image to black and white and making it thinner so that each ridge is shown as a one-pixel line. Often, before extracting the ridgelines, the image is enhanced by applying directional filters, to reduce the presence of noise. [43][47]

B. Vein Recognition

Vein recognition is a biometric identification technique that uses an individual's unique vein patterns in their body, generally in their hands or fingers, to authenticate their identity. Vein patterns are very distinguishable and difficult to copy, making them an effective biometric identification.

Finger vein identification biometrics relies on the analysis of vein patterns within an individual's hand. An attester terminal equipped with a near-infrared LED light source and a monochrome camera is used to capture these patterns. Due to the light absorption properties of hemoglobin in the blood, the veins manifest as a complex network of distinctive lines. The camera captures this image, converting it into raw data which is digitized and stored within a database of comparable imagery.

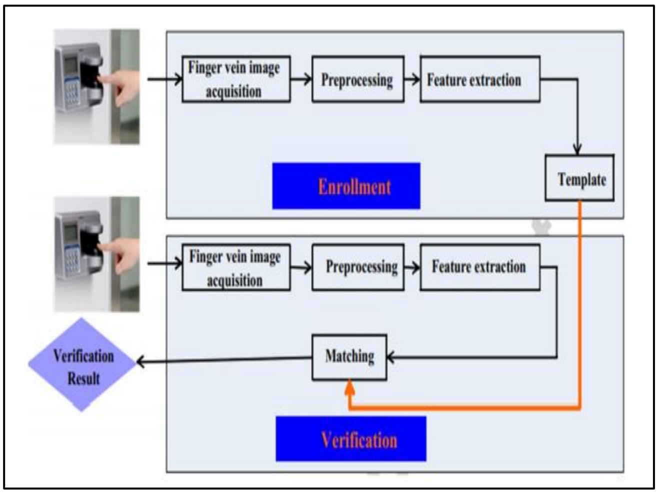

Fig 5 Basic Framework for Finger Vein Recognition [8]

➢ *History and Evolution:*

The history of vein recognition technology is a brief one, but it's no less significant. Discovery of vein recognition technology dates back to 1991, and it has been revolutionizing biometrics since as it is a highly reliable technique due to its live detection technology. [7][51]

Along with Finger vein technology, hand vein recognition technology is also present which increases the accuracy.

One major advantage of this technology is that the veins are present inside the hand/finger, and hence cannot be fabricated and it is a highly stable biometric trait [39]

➢ *Limitations [15]:*

- Distinctiveness and Reliability: Lack of sufficient medical evidence for the distinctiveness and stability of finger vein patterns.
- Image Acquisition: High cost of finger vein acquisition devices, limiting widespread adoption.
- Finger Displacement: Difficulty in handling 3-dimensional posture changes during image acquisition, compared to 2-dimensional changes.
- Lack of Large-Scale Applications: Limited practical applications of finger vein recognition, particularly on a large scale.
- Need for Improvement: The need for a large-scale public finger vein database to evaluate methods.

➢ *Advancements:*

Dai et al [34] developed a method to capture higher quality finger vein images by using nonuniform infrared light intensity rather than uniform intensity. This resulted in more uniform finger brightness, clearer vein patterns, and increased numbers of useful features compared to images from a common device. Specifically, their method decreased the standard deviation of gray levels by 48.4% on average. It also increased the total detectable vein length by 44.1% and the number of vein bifurcations by 31.4% on average. The improved images provide more identifying features for fingerprint authentication.

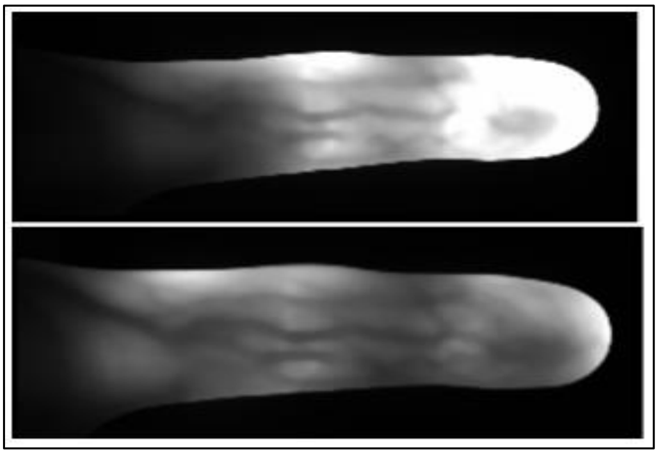
Fig 6 (a) with (b) and without non Uniform Intensity IR Light

- Huang et al [23] proposed a method to correct finger posture changes in finger vein images for biometric recognition. They identified and analyzed 6 types of posture changes and their effects on the vein patterns in 2D images. To normalize the images, they developed a model to reconstruct a 3D normalized finger shape from the 2D images.

➢ *State-of-the-Art*

Finger vein recognition is gaining attention in biometrics due to its convenience and high security. Zhang et al. [1] introduce a novel approach, the joint Bayesian framework, using partial least squares discriminant analysis (PLS-DA) for effective recognition. The framework has three stages:

- Creating robust feature descriptions using Gabor filters to detect finger vein lines and orientation, turning them into local patch histograms.
- Employing PLS-DA-based discriminant feature mapping (PLS-DA-FM) to transform basic features into a more compact, differentiating representation guided by supervision.
- Building a Bayesian model considering combined pairs of finger vein features to assess their similarity. [1]

C. *Iris Recognition*

Iris Recognition is a biometric technique used for identifying individuals by analyzing distinct patterns found within the circular area of the eye's pupil. An individual's iris is very unique to them, which is why it serves as a highly effective form of biometric authentication.

A black and white video camera aided by a low-level light to focus is used to capture a sharp image of the iris. Then a frame from this video is digitized and stored into a database which can be referred to during authentication by matching the two templates. [29]

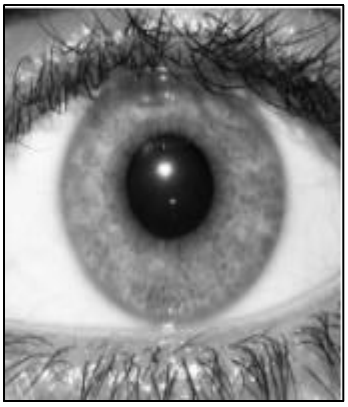
Fig 7 (a) Original Image of Eye

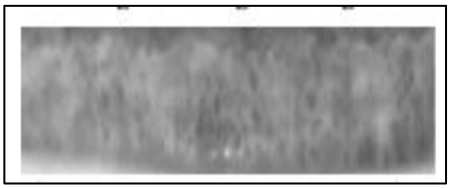
Fig 7 (b) Isolated Image of Iris [42]

➢ *History and Evolution:*

- In 1936, Frank Burch introduced the concept of identifying individuals based on their unique iris patterns.
- In 1985, Dr. Leonard Flom and Dr. Aran Safir established that no two irises are identical.
- In 1995, The first commercial unit developed and tested by The Defense Nuclear Agency became available. [16]

➢ *Limitations:*

- Most current techniques focus on frontal view iris images under ideal conditions.
- Current techniques are not able to handle varying iris-to-camera distances well.
- Some techniques require manual/semi-automated training which limits real-world applicability
- Segmentation is a prerequisite for some approaches, but failed segmentation leads to inaccurate results. Robust segmentation is still a challenge, especially with non-ideal images.
- Factors like eyelids, eyelashes, and shadows interfere with effective iris segmentation. [28]

➢ *Advancements:*

Vanaja et al [26] focused on optimizing iris recognition even with the presence of noise and other factors. Successfully worked on a sample of an image of a moving person's iris from UBIRIS database.

➢ *State-of-the-Art*

Principal Component Analysis (PCA) is a widely-known method in statistics, used in fields like signal and image processing, and communications when dealing with linear models. It's valuable for simplifying complex data.

PCA compresses images, similar to simplifying a map while keeping important landmarks visible. It works by transforming data into a new coordinate system, highlighting the most significant differences. PCA is versatile, helpful for large datasets like iris images. [48]

D. Retina Scanning

Retina scanning uses the distinctive patterns of blood vessels in the retina of the eye to identify and verify people. The retina is a thin layer of tissue located at the back of the eye that includes light-sensitive cells. It's complicated circulatory network generates unique patterns that stay relatively constant throughout time.

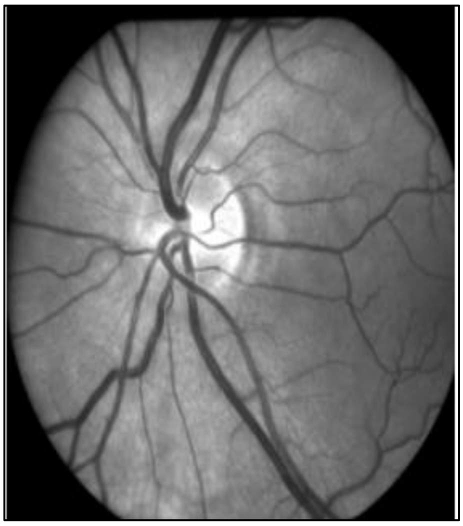

Fig 8 Fundus Camera Retina Image of a Left Eye

➢ *History and Evolution:*

In 1935, Dr. Carleton Simon and Dr. Isodore Goldstein established with their studies that each retina has a unique blood vessel pattern.

They later suggested the use of photographs of these unique patterns for identification.

In 1950s, Dr. Paul Tower discovered that even amongst identical twins this blood vessel pattern is distinguishable.

The first prototype of a retina scanning device was developed in 1981 (by EyeDentify) which used infrared light to illuminate blood vessels for acquisition of the image. [31]

➢ *Limitations:*

- Conditions like cataract can cause errors in the identification process. [6]
- Perceived Health Concerns: Some believe retinal identification may harm the eyes, despite low light levels used for scanning, especially in less familiar applications.
- Outdoor vs. Indoor Performance: Small pupils can reduce scanning accuracy due to less light reaching the retina, leading to errors in varying light conditions.
- Ergonomic Challenges: Using the retina scanning device requires precise positioning.
- High Sensor Cost: Retina scanning relies on costly cameras, making the system more expensive. [46]

➢ *Advancements:*

- Multimodal approach proposed by Usher et al [35] is a hybrid of iris recognition and retina scanning which can be used to improve accuracy.
- Liveness detection approach for this technique can be highly effective as it is naturally anti-spoof. [11]
- Meng et al [14] proposed an approach to efficiently implement this technology in mobile phones.

➢ *State-of-the-Art*

Using near-infrared images for retina recognition is accurate but costly and less accepted. An algorithm employing affordable visible light imaging captures green channel images under regular lighting. It identifies the fovea, forms a raw waveform, and enhances contrast. Matching utilizes Fourier transforms for specific vascular patterns.

Assessment with 58 subjects yielded false accept rates averaging below 0.02 with filtered signals and under 0.01 without, showcasing robustness without extensive adjustments. This method addresses adoption challenges compared to infrared, offering economical and flexible imaging. It introduces waveform contrast normalization and frequency isolation, enhancing retina biometrics. Future research will examine aging, illness, and sensor-specific optimizations. [37]

E. *Facial Recognition*

Face recognition is a biometric identification technology that verifies and authenticates an individual's identity by utilizing distinctive aspects of their face. It is based on the concept that the human face has distinct and recognizable traits that computer algorithms can collect and analyze.

➢ *History and Evolution:*

Faces have always been a primary factor in identifying a human being. Slowly and gradually other ways of using facial features to identify came into practice such as portraits, and eventually photographs that were used by the British police in 1840s to identify individuals. [40]

In 1967, the first experiments with semi-automated computer based facial recognition were took place.

1970s saw an increase in accuracy with 21 facial markers to differentiate.

In Early 2000s law enforcement started using facial recognition, including the identification of Osama Bin Laden using this technology.

Facebook came up with its Deep Face photo tag feature in 2014. [3]

Since then facial recognition has become a big part of the technology we use everyday that includes mobile phones most of which are equipped with biometric recognition technologies.

➢ *Limitations:*

- Environmental Factors: Lighting and sweat on the face can reduce face recognition accuracy.
- Age and Variability: Age-related changes, facial expressions, and head positions can cause face recognition errors.
- Lack of Stability: The changes in face, including facial hair growth, affects face recognition reliability. [13]

➢ *Advancements:*

Deb et al [4] proposed a method that can age deep face features to enhance cross age-face recognition in identifying missing children.

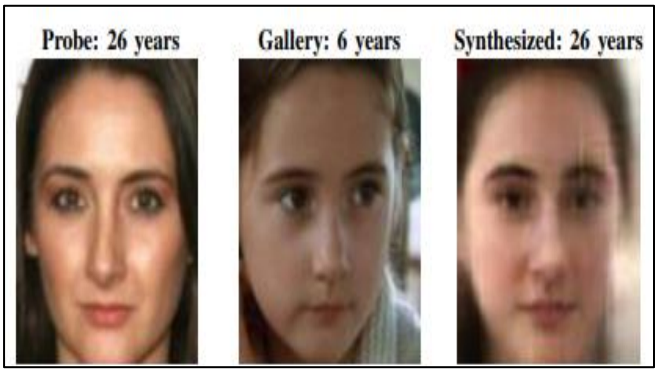

Fig 9 Comparison of Synthesized and Probe Image [4]

➢ *State-of-the-Art*

- 3D face recognition utilizing depth cameras, stereo imaging, or model fitting has grown as a way to handle pose variation and spoofing.
- Hybrid approaches combine multiple modalities like visible light, thermal infrared, depth, and video to improve robustness.
- Innovations like face frontalization, address pose challenges
- Attention mechanisms focus neural networks on discriminative regions versus whole faces. This improves efficiency and accuracy.
- Video and 3D capabilities have expanded face recognition into motion-based recognition and anti-spoofing. [10]

F. *Hand Geometry*

Human hands are distinctive features, although there is not enough study to state that each hand has unique geometry, this technique can be used in identification of a small group of people. The measurements of length, width, thickness of fingers and palm, and broadness of the palm can be used to distinguish individuals.

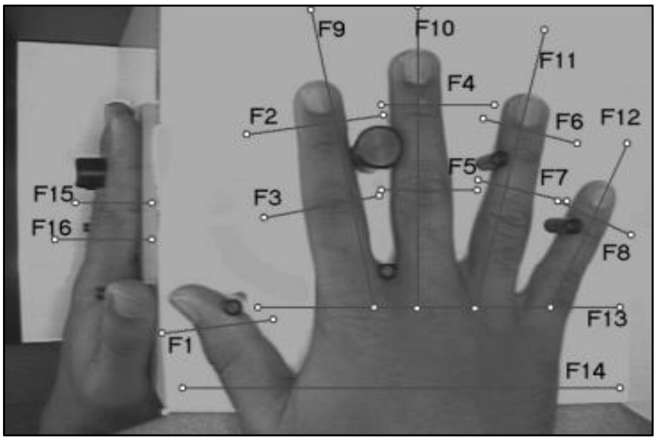

Fig 10 Silhouette of an Image of a Hand [24]

A camera is used to capture a silhouette image of the hand. To ensure correct placement of the hand 5 pegs are used to place the hand in the correct position for the image to be taken.

➢ *History and Evolution*

- In 1971, US Patent Office patented a device for measuring hand characteristics for identification.
- In 1996 during Olympic games in Atlanta, hand geometry was used for access control in the Olympic village.
- In 2004, this characteristic was formally recognized. It’s has been used in multiple instances because of its low cost and easy enrollment features. [24]

➢ *Limitations:*

- Uniqueness: Debate exists on hand shape as a unique identifier in large populations. Some high-accuracy studies use controlled, offline data, lacking real-world variability and user manipulation challenges.
- Deformations and Misalignment: In images, hands can deform unpredictably, especially with untrained users, causing alignment issues and authentication failures.
- Vulnerability to Spoofing: Hand geometry systems may be tricked by fake hand images, harming security and accuracy. [33]
- Variation in age might bring change to the geometry, hence its not a stable characteristic. [13]

➢ *Advancements:*

Singh et al [32] proposed a method that includes skin color as a distinguishing factor along with hand geometry, which can improve accuracy and make it more distinctive.

➢ *State-of-the-Art*

Hand geometry recognition utilizes the geometric shape and dimensions of the human hand as a biometric modality for personal authentication. Pavešić et al. [41] studies hand geometry recognition methods and systems. Hand geometry, despite some uniqueness limitations, offers advantages like easy data collection and user acceptance compared to more invasive biometrics like fingerprints.

The authors review hand, finger, and palm geometry in research prototypes and commercial systems, measuring aspects like finger size, shape, and palm area. Matching involves statistical classifiers or elastic models to compare feature sets, including Bayesian matching, neural networks, and flexible hand shape verification. Accuracy varies based on data size, features, and matching methods.

They highlight multimodal systems combining hand geometry with palm print biometrics for better accuracy and reliability. One suggested system combines finger and palm geometry with palm print textures, determining an overall similarity measure for access decisions.

On a 110-user database, the multimodal system achieved a 0.41% equal error rate and a 0.75% minimum total error rate. Unimodal hand geometry error rates ranged from 5-33%, while palm print error rates were 0-8%. This shows the benefits of combining biometrics. Future work could include adding fingerprint data, as all modalities can be extracted from a single hand image.

V. COMPARISON OF BIOMETRIC TECHNIQUES

➢ *To Compare Biometric Techniques the following Factors can be used:*

- *False Acceptance Rate (FAR): This percentage indicates how often a biometric system recognizes an unauthorized person as an authorized one. In simpler terms.*
- *False Rejection Rate (FRR): This percentage represents how often the biometric system makes the mistake of rejecting an authorized person and denying them access.*
- *Generalized False Rejection Rate (GFRR): This measure considers everyday conditions and user errors, offering a more practical view of how often the system might wrongly reject someone.*
- *Failure to Enroll (FTE): This percentage reflects the number of individuals who can't register in the biometric system, preventing them from using it.*
- *Risk of Spoof: This factor assesses how vulnerable the system is to being tricked or bypassed by fraudulent methods.*
- *Live Sample Detection: Indicates if the system can distinguish between a living sample and a fake or non-living sample.*
- *User Acceptance: Assesses people's willingness to embrace biometric technology, considering their attitudes, cooperation, and any concerns or misunderstandings.*
- *Contact Requirement: Tells us if physical contact with the biometric device is necessary for identification, if yes how much.*
- *Stability: Checks if the biometric trait used remains stable over time and is unaffected by external factors*
- *Risks: Covers potential issues that could harm the biometric system's operation and application.*
- *Collectability: Evaluates how easily biometric samples are gathered during enrollment.*

- *Cost: Cost evaluates the financial aspects of implementing and maintaining a biometric authentication system. The following factors affect cost [44]:*

✓ Biometric Capture Hardware
✓ Back-End Processing Power
✓ Research and Testing
✓ Installation
✓ Mounting, Installation, Connection, and User System Integration
✓ User Education
✓ Exception Processing
✓ Productivity Losses
✓ System Maintenance

- Speed: The efficiency of a biometric system in rapidly processing authentication requests, crucial for minimizing delays and ensuring quick access approval, particularly in high-traffic settings. [12]
- Usability: User-friendliness of the signature tool (both software and hardware) and how it affects the user experience.
- Maintenance: Care required to keep the system working well for a long period of time.
- Performance: Attainable accuracy and speed along with the needed resources and environmental factors impacting them.
- Accuracy: The accuracy of the system to identify a user.
- Security level: The level of security the system provides in terms of higher accuracy and stronger differentiation of users.

Table 1 Comparison of Biometric Techniques using the above-Mentioned Factors. [6, 9, 12, 17, 19, 30, 38, 44, 45]

Biometric Identification method	**Fingerprint (Multispectral optics)**	**Vein**	**Iris**	**Retina**	**Face**	**Hand geometry**
FAR (%)	10^{-5}	10^{-2}	10^{-7}	10^{-2}	10^{-2}	10^{-2}
FRR (%)	10^{-3}	10^{-2}	10^{-4}	10^{-3}	10^{-2}	10^{-2}
GFRR (%)	10^{-1}	1	10^{-1}	NA	1-5	1
FTE (%)	10^{-1}	1	1	NA	1	0,10
Risk of spoof	Very Low	Low	Very Low	Very Low	Medium-Low	Medium-Low
Live sample detection	Changes rarely	Vulnerable	High	Low	Medium	Medium
Acceptability	High	Medium	Low	Low	High	Medium
Contact requirement	Small surface	Small surface	None	None	None	Contact of palm with the sensor
Stability	Changes rarely	Does not change	Does not change	Changes rarely	Changes often	Changes rarely
Risks	Not enough experience	Low availability	Might not be accepted by people	Rejected technology	Vulnerable	Vulnerable
Collectability	Medium	Medium	Medium	Low	High	High
Cost	Medium	Medium	High	High	medium	High
Speed	High	High	Medium	Medium	High	Medium
Usability	Easy	Easy	Easy	Difficult	Difficult	Medium
Maintenance	Medium-High	Medium	Medium	Medium	Medium	Medium
Performance	High	Medium	High	High	Low	Medium
Accuracy	Medium	High	High	High	Medium	High
Security level	Low	High	Medium	Medium	Low	Medium

VI. LATEST TRENDS

Multimodal biometric systems enhance security by using multiple biometric traits for identification. These systems capitalize on the strengths of different biometric characteristics, such as fingerprints, facial features, and voice patterns, to achieve more accurate and reliable identification results. By combining these traits, the system can overcome limitations inherent in single-modal systems, offering improved accuracy and robustness in various applications, including access control and identity verification.

A. Multimodal Categories

Multi-biometric systems fall into two main categories: synchronous and asynchronous. In synchronous systems, multiple biometrics are used together during a single authorization process. In contrast, asynchronous systems use two biometric technologies one after the other [36]. Multimodal biometric systems can work in three different ways [20]:

- Serial Mode (cascade mode) - each biometric is checked one by one before moving on to the next. This can speed up the recognition process by narrowing down the possible identities before using the next biometric.

- Parallel Mode - data from multiple biometrics are used simultaneously for recognition, and then the results are combined for the final decision.
- Hierarchical Mode - individual classifiers are combined in a tree-like structure. This mode is preferred when dealing with many classifiers.

B. Multi-Biometrics Integration

Multiple biometric traits are used in identification to further improve reliability and security.

- *Multi-Sensor Systems:*

Multi-sensor systems are designed to gather information about a person's unique traits using different kinds of sensors. Imagine you're dealing with fingerprints. Instead of just one type of sensor, like the kind that uses light or the one that measures electrical signals, you use different ones – say, optical and capacitive sensors. These different sensors pick up additional details that, when combined, provide a more complete picture of the fingerprint. To make all this data work together, there's a technique that helps merge it. This technique works at the level of the sensors themselves [25].

- *Multi-Modal Systems:*

In multi-modal systems, more than just one trait is used to figure out who someone is. Picture someone's face and their voice – both can be used together to confirm their identity. Now, this might sound a bit more expensive because you need different gadgets for each trait, but it really pays off because the results are a lot better. Using more traits means the system can be surer about who it's dealing with.

- *Multi-Instance Systems:*

Multi-instance systems gather lots of examples of a single trait. For example, when it comes to recognizing someone's iris (that's the colorful part of the eye), you can take pictures of the left and right sides. Or when it's fingerprints, you might combine images from a few different fingers of the same person. To keep things simple and save costs, you could use just one sensor to take these pictures one after the other. This way, you don't need to buy many sensors or add extra bits to process the information [27].

- *Multi-Sample Systems:*

Think of multi-sample systems as taking extra pictures. Instead of just one snap, you get a few. Let's say you're looking at someone's face – along with a straight-on shot, you also get pictures of their face from the sides. Or when you're dealing with fingerprints, you take several pictures of the same finger or a few different times. This can help when a single picture might not work so well. However, doing this might need more sensors or make the person wait a bit longer to get everything done.

- *Multi-Algorithm Systems:*

Multi-algorithm systems try different ways of looking at the same trait. Imagine you're trying to recognize someone's face. You can use different methods to find the features that make them unique. Then, you put all these different methods' results together and make a final decision. These systems are a bit like using different tools to solve a puzzle. They're good because you don't need to buy more gadgets, but they can get a bit tricky because you're using lots of different ways to figure things out [25].

- *Hybrid Systems:*

A hybrid system is like a mix of different approaches. Think of it as putting two or more things together to get the best of both. For example, you could use one way of recognizing faces along with another way for fingerprints. If you use different gadgets to take pictures, it becomes a multi-gadget system. And if you take pictures of a person's trait a few times, it becomes a multi-example system.

Both hybrid and multi-modal systems can use more than one way to do things, but the other systems can work well with just one way [21].

VII. CONCLUSION

Biometric-based authentication has made remarkable progress over the past few decades, evolving from early fingerprint recognition to advanced iris, facial and multimodal techniques. This paper provided a comprehensive review of major physiological biometrics, including their history, evolution, principles, applications, limitations, and recent advances.

Each biometric technology has its own strengths and weaknesses, with no single modality being universally superior. Multimodal systems that fuse multiple biometrics are emerging as a promising approach to overcome the limitations of unimodal systems and achieve higher accuracy. Ongoing research on enhancing accuracy, security, user convenience and spoof resistance continues to expand the frontiers of biometrics.

Real-world deployment of biometrics faces challenges like user acceptance, cost, security threats and ethical implications which must be addressed through reasonable safeguards and transparency. With careful consideration of these factors, biometrics can play a major role in revolutionizing identity verification across domains, balancing security, and convenience.

This review covered key developments, comparisons, trends and challenges to provide a holistic overview of the state-of-the-art in biometric authentication. It adds to the knowledge base for researchers, developers and policy makers working to harness biometrics for secure and seamless recognition of individuals based on their intrinsic bodily characteristics. Further research can build on this foundation to advance biometric science and engineering for the future.

REFERENCES

[1]. L. Zhang et al., "A Joint Bayesian Framework Based on Partial Least Squares Discriminant Analysis for Finger Vein Recognition," in IEEE Sensors Journal, vol. 22, no. 1, pp. 785-794, 1 Jan.1, 2022, doi: 10.1109/JSEN.2021.3130951.

[2]. Alsaadi, Israa. (2021). Study On Most Popular Behavioral Biometrics, Advantages, Disadvantages And Recent Applications : A Review. 10.13140/RG.2.2.28802.09926.

[3]. Sullivan, E., 2021. Facial Recognition Technology. Economic Affairs Interim Committee, Montana State Legislature

[4]. Deb, D., Aggarwal, D., & Jain, A. K. (2021). Identifying Missing Children: Face Age-Progression via Deep Feature Aging. 2020 25th International Conference on Pattern Recognition (ICPR). doi:10.1109/icpr48806.2021.9411913

[5]. Fakiha, B.S., 2020. How technology has improved forensic fingerprint identification to solve crimes. International Journal of Advanced Science and Technology, 29(5), pp.746-752.

[6]. Dargan, S. and Kumar, M., 2020. A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications, 143, p.113114.

[7]. Wu, W., Elliott, S. J., Lin, S., Sun, S., & Tang, Y. (2019). A review of palm vein recognition. IET Biometrics. doi:10.1049/iet-bmt.2019.0034

[8]. Shaheed, K., Liu, H., Yang, G., Qureshi, I., Gou, J., & Yin, Y. (2018). A Systematic Review of Finger Vein Recognition Techniques. Information, 9(9), 213. doi:10.3390/info9090213

[9]. Shaheed, K., Liu, H., Yang, G., Qureshi, I., Gou, J., & Yin, Y. (2018). A Systematic Review of Finger Vein Recognition Techniques. Information, 9(9), 213. doi:10.3390/info9090213

[10]. Mahmood, Z., Muhammad, N., Bibi, N. and Ali, T., 2017. A review on state-of-the-art face recognition approaches. Fractals, 25(02), p.1750025.

[11]. Shaydyuk, N. K., & Cleland, T. (2016). Biometric identification via retina scanning with liveness detection using speckle contrast imaging. 2016 IEEE International Carnahan Conference on Security Technology (ICCST). doi:10.1109/ccst.2016. 7815706.

[12]. Otti, C. (2016). Comparison of biometric identification methods. 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI). doi:10.1109/saci.2016.7507397

[13]. Tiwari, S., Chourasia, J.N. and Chourasia, V.S., 2015. A review of advancements in biometric systems. International Journal of Innovative Research in Advanced Engineering, 2(1), pp.187-204.

[14]. Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the Development of Biometric User Authentication on Mobile Phones. IEEE Communications Surveys & Tutorials, 17(3), 1268–1293. doi:10.1109/comst.2014.2386915

[15]. Yang, L., Yang, G., Yin, Y. and Zhou, L., 2014. A survey of finger vein recognition. In Biometric Recognition: 9th Chinese Conference, CCBR 2014, Shenyang, China, November 7-9, 2014. Proceedings 9 (pp. 234-243). Springer International Publishing.

[16]. Shah, N. and Shrinath, P., 2014. Iris recognition system–a review. International Journal of Computer and Information Technology, 3(02), pp.321-327.

[17]. Saini, R. and Rana, N., 2014. Comparison of various biometric methods. International Journal of Advances in Science and Technology, 2(1), pp.24-30.

[18]. Jani, R., & Agrawal, N. (2013). A Proposed Framework for Enhancing Security in Fingerprint and Finger-Vein Multimodal Biometric Recognition. 2013 International Conference on Machine Intelligence and Research Advancement. doi:10.1109/icmira.2013.93

[19]. Saini, H. and Garg, K., 2013. Comparative Analysis of Various Biometric Techniques for Database Security. IJSR (International journal of Science and Research) Vol, 2, pp.45-51.

[20]. G. Amirthalingam, "A Multimodal Approach for Face and Ear Biometric System," International Journal of Computer Science Issues (IJCSI), vol. 10, no. 5, pp. 234-241, 2013.

[21]. D. T. Meva and C. K. Kumbharana, "Comparative Study of Different fusion techniques in multimodal biometric authentication," International Journal of Computer Applications, vol. 66, no. 19, 2013.

[22]. Jain, S., Gupta, S. and Thenua, R.K., 2012. A review on advancements in biometrics. Int J Electron Comput Sci Eng, 1, pp.853-9.

[23]. Huang, B., Liu, S., & Li, W. (2012). A finger posture change correction method for finger-vein recognition. 2012 IEEE Symposium on Computational Intelligence for Security and Defence Applications. doi:10.1109/cisda.2012.6291530

[24]. Fotak, T., Koruga, P. and Baca, M., 2012. Trends in hand geometry biometrics. In Central European Conference on Information and Intelligent Systems (p. 319). Faculty of Organization and Informatics Varazdin.

[25]. H. AlMahafzah and M. Z. AlRwashdeh, "A Survey of Multibiometric Systems," International Journal of Computer Applications vol. 43, no. 15, pp. 36-43, 2012.

[26]. Chirchi, V.R.E., Waghmare, L.M. and Chirchi, E.R., 2011. Iris biometric recognition for person identification in security systems. International Journal of Computer Applications, 24(9), pp.1-6.

[27]. M. S. Ahuja and S. Chabbra, "A Survey of Multimodal Biometrics," International Journal of Computer Science and its Applications, vol. 1, no. pp. 157-160, 2011.

[28]. Birgale, L., & Kokare, M. (2011). Recent Trends in Iris Recognition. Pattern Recognition, Machine Intelligence and Biometrics, 785–796. doi:10.1007/978-3-642-22407-2_29

[29]. Gawande, U., Zaveri, M. and Kapur, A., 2010. Improving iris recognition accuracy by score based fusion method. arXiv preprint arXiv:1007.0412.

[30]. Aboalsamh, H., 2010, July. Recent advancements in biometrics: vein and fingerprint authentication. In 14th WSEAS International Conference on Computers (Part of the 14th WSEAS CSCC Multiconference) (pp. 459-462).

[31]. Zibran, M.F., 2009. Eye based authentication: Iris and retina recognition. Technical Report# 2011-04, University of Saskatchewan.

[32]. Singh, A. K., Agrawal, A. K., & Pal, C. B. (2009). Hand geometry verification system: A review. 2009 International Conference on Ultra Modern Telecommunications & Workshops. doi:10.1109/icumt.2009.5345652

[33]. Duta, N. (2009). A survey of biometric technology based on hand shape. Pattern Recognition, 42(11), 2797–2806. doi:10.1016/j.patcog.2009.02.007

[34]. Y. Dai, B. Huang, W. Li and Z. Xu, "A Method for Capturing the Finger-Vein Image Using Nonuniform Intensity Infrared Light," 2008 Congress on Image and Signal Processing, Sanya, China, 2008, pp. 501-505, doi: 10.1109/CISP.2008.654.

[35]. Usher, D., Tosa, Y. and Friedman, M., 2008. Ocular biometrics: simultaneous capture and analysis of the retina and iris. In Advances in Biometrics: Sensors, Algorithms and Systems (pp. 133-155). London: Springer London.

[36]. M. Deriche, "Trends and Challenges in Mono and Multi biometrics," presented at the Image Processing Theory, Tools and Applications, 2008. IPTA 2008. First Workshops on, Sousse, 2008. pp. 1-9.

[37]. Borgen, H., Bours, P., & Wolthusen, S. D. (2008). Visible-Spectrum Biometric Retina Recognition. 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing. doi:10.1109/iih-msp.2008.345

[38]. Hashimoto, J. (n.d.). Finger Vein Authentication Technology and Its Future. 2006 Symposium on VLSI Circuits, 2006. Digest of Technical Papers. doi:10.1109/vlsic.2006.1705285

[39]. Yuhang Ding, Dayan Zhuang, & Kejun Wang. (n.d.). A study of hand vein recognition method. IEEE International Conference Mechatronics and Automation, 2005. doi:10.1109/icma.2005.1626888

[40]. Gates, K., 2004. The past perfect promise of facial recognition technology. ACDIS Occasional Paper.

[41]. Pavešić, N., Ribarić, S. and Ribarić, D., 2004. Personal authentication using hand-geometry and palmprint features–the state of the art. Hand, 11, p.12.

[42]. Daouk, C.H., El-Esber, L.A., Kammoun, F.D. and Al Alaoui, M.A., 2002. Iris recognition. In IEEE ISSPIT (No. 4, p. 558).

[43]. Senior, A., A combination fingerprint classifier, IEEE Trans. on Pattern Analysis Machine Intelligence, 23(10):1165–1174, 2001.

[44]. Liu, S. and Silverman, M., 2001. A practical guide to biometric security technology. IT Professional, 3(1), pp.27-32.

[45]. Scheuermann, D., Schwiderski-Grosche, S. and Struif, B., 2000. Usability of biometrics in relation to electronic signatures. Sankt Augustin: GMD-Forschungszentrum Informationstechnik.

[46]. Jain, A., Bolle, R. and Pankanti, S. eds., 1999. Biometrics: personal identification in networked society (Vol. 479). Springer Science & Business Media.

[47]. Chong, M.M., Tan, H.N., Jun, L. and Gay, R.K., 1997. Geometric framework for fingerprint image classification. Pattern Recognition, 30(9), pp.1475-1488.

[48]. Wildes, R.P., 1997. Iris recognition: an emerging biometric technology. Proceedings of the IEEE, 85(9), pp.1348-1363.

[49]. L. O'Gorman, "Fingerprint Verification," Fingerprint Verification | SpringerLink. https://link.springer.com/chapter/10.1007/0-306-47044-6_2

[50]. Karu, K. and A.K. Jain, Fingerprint classification, Pattern Recognition, 29(3):389–404, 1996.

[51]. MacGregor, P., & Welford, R. (1992). VEINCHECK LENDS A HAND FOR HIGH SECURITY. Sensor Review, 12(3), 19–23. doi:10.1108/eb007880

[52]. Kawagoe, M. and A. Tojo, Fingerprint pattern classification, Pattern Recognition, 17(3):295–303, 1984.

[53]. Grasselli, A., On the automatic classification of fingerprint—Some consideration of the linguistic interpretation of pictures, in Methodologies of Pattern Recognition, S.Watanabe, ed., Academic Press, 1969, pp. 253–273.

[54]. Stock, R.M. and C.W. Swonger, Development and evaluation of a reader of fingerprint minutiae, Cornell Aeronautical Laboratory, Technical Report CAL no. XM-2478-X-1:13– 17, 1969.