Survey on 2D and 3D Physiological Biometric Traits for Human identification

G Divya[1], A S Mamatha[2], H C Nagaraj[3], Prasanna G Paga[4]

[1]Department of Electronics and Communication Engineering, Assistant Professor, Nitte Meenakshi Institute of Technology, Bengaluru, India

[2]Department of Electronics and Communication Engineering, Associate Professor, NITTE (Deemed to be University), NMAM Institute of Technology, Nitte, Karnataka, India

[3]Department of Electronics and Communication Engineering, Principal, Nitte Meenakshi Institute of Technology, Bengaluru, India

[4]Department of Electronics and Communication Engineering, Associate Professor, Nitte Meenakshi Institute of Technology, Bengaluru, India

Corresponding Author:

A S Mamatha

Associate Professor, Department of Electronics and Communication Engineering, NITTE (Deemed to be University), NMAM Institute of Technology, Nitte, Karnataka, India

Email: mamathag_12@rediffmail.com

Keywords:

Biometric Identifier
3D Finger Knuckle
Finger knuckle trait
physiological traits
Finger geometry patterns

ABSTRACT

Biometric-based personal authentication systems are more reliable and user friendly, overruns the traditional personal authentication systems such as knowledge-based system and token-based system. Individuals are verified and identified using biometric technology based on their biological or behavioural traits .The physiological biometric traits gets abraded due to aging and massive work, while the behavioural biometric traits are having high variations due to external factors such as fatigue, mood etc. Among the physiological biometric traits, Finger geometry patterns are widely deployed authentication system reason being its stability, user acceptability and uniqueness. Recent trends in Biometrics attempt to incorporate 3D domain, since 3D images are usually more robust and illumination invariant compared to 2D intensity domain.

1 INTRODUCTION

To access a variety of resources, from computer systems to research facilities and locations like college campuses, to nuclear plants, we frequently need to authenticate our identities or the identities of others. All security systems are based on access control; to discriminate between law-abiding citizens and criminals, the appropriate individuals should be permitted entry while the inappropriate individuals should be barred. Authentication is the process of allowing only authenticated individuals to access the designated protected resources and locations [1-2]. Traditional authentication systems are based on "What you know" (Knowledge Based Systems), which includes Passwords and PINs or anything else you can remember and write, and "What you have" (Token Based Systems), which includes physical authentication devices. The below points outline the primary issues or deficiencies associated with authentication systems based on passwords, smart cards, or password tokens: Passwords and personal identification numbers (PINs) function well as long as they remain impervious to unauthorized guessing attempts. The act of sharing passwords presents a significant issue. While password tokens or smart cards are not as easily shared as passwords, they are nonetheless susceptible to theft or loss [3]. The pilfered cards has the potential to be utilized by an unauthorized individual in order to obtain access to various resources.

There are several vulnerabilities and challenges that are inherently linked to what you know and what you have Authentication Systems. The inherent limitations of Authentication Systems prevent them from accurately discerning the origin of an authenticator, namely if it originates from a device that has been guessed, shared, or stolen [4]. These systems provide a significant potential for unauthorized individuals or criminal entities to readily breach the security measures and get access to the safeguarded resources. To effectively tackle these concerns, it is imperative to implement a more streamlined and robust Authentication System. The proposed solution is an authentication system based on biometrics, specifically known as "What You Are" [5]. The term "Biometric" is etymologically derived from the combination of two Greek terms, namely "bios" which pertains to life, and "metros" which denotes measurement. The process of automatically verifying and identifying an individual's identification is accomplished by analyzing one or more distinct physiological or behavioral features [6-8]. The primary benefits of biometric systems include: The password, in the case of forgery, or identity cards, in the event of misplacement, are both examples of items that are not susceptible to fraudulent replication or accidental loss [9]. The differentiation between authentic individuals and imposters is consistently established by the discernment of unique attributes, necessitating the actual presence of the individual in question. Biometric systems provide enhanced reliability and user-friendliness. A biometric system may be described as a technological tool utilized to ascertain the identity of an individual by quantifying one or many physiological or behavioral attributes.

The term "biometric modality" is used to describe the physiological or behavioral measurements obtained from an individual for the purpose of authentication. The Biometric modalities that are widely acknowledged and approved on a global scale include Fingerprints, Palm prints, Hand geometry, Finger knuckle prints, Facial recognition, Iris scans, Retinal scans, Ear recognition, Voice recognition, Signature analysis, and Keystroke dynamics. There are two different categories for biometric systems as shown in Figure 1, Behavioral and

physiological biometrics. The physical qualities of a person are represented by their physiological biometric traits, while their behavioral biometric traits are their behavioral characteristics [10]. While the behavioral biometric features are very variable due to outside influences like weariness, mood, and other factors, the physiological biometric traits deteriorate with age and heavy work [11]. Finger geometry patterns are one of the physiological biometric qualities that are frequently used in authentication systems because of their stability, user acceptance, and uniqueness. Finger knuckle traits get worn less under finger geometry patterns because they are exposed to less intense work.

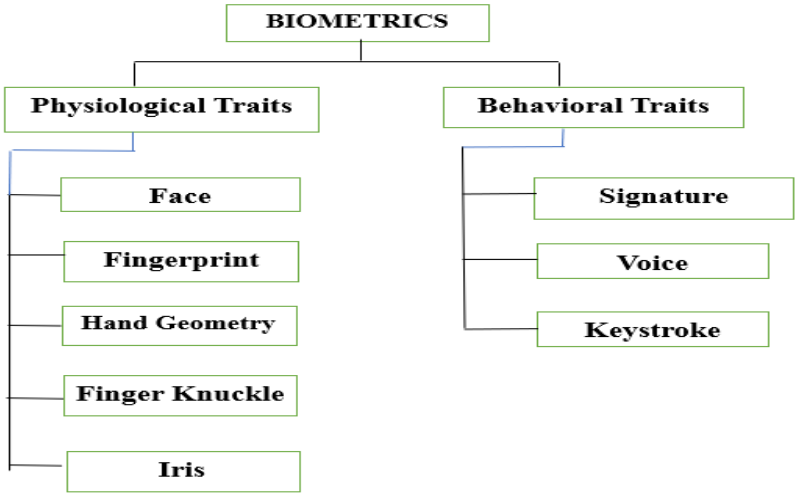

Figure 1.Biometric Classification

In the realm of authentication systems, biometric traits emerge as paramount, harnessing unique physiological and behavioral characteristics to identify individuals with unparalleled precision and security. This paradigm shift from conventional authentication methodologies, such as passwords and physical tokens, to biometrics, underscores the critical vulnerabilities namely theft, loss, and unauthorized sharing—associated with traditional systems. By leveraging intrinsic attributes, including but not limited to fingerprints, iris patterns, facial geometry, and voice signatures, biometric authentication systems transcend these limitations [12]. They offer enhanced security, increased user convenience, and a higher reliability level for identity verification. This innovative approach not only addresses the inherent deficiencies of knowledge-based and token-based systems but also marks a significant technological advancement in securing access control mechanisms across a multitude of sectors. As such, biometric technologies have become indispensable in modern security architectures, providing a seamless, non-intrusive, and highly accurate method for ensuring the integrity of personal identification and access systems.

The finger knuckle trait represents an innovative biometric identifier, capitalizing on the unique and stable patterns found on the human finger's knuckle regions. These patterns, resistant to wear and environmental changes, offer a secure and distinctive means for human identification. Utilizing non-intrusive imaging technologies, finger knuckle recognition systems capture and analyze these intricate patterns, providing a reliable method for verifying individual identities

[13]. With advantages such as high uniqueness, resilience to forgery, and ease of acquisition, the finger knuckle trait is emerging as a promising solution in the realm of biometric security, finding applications in access control, forensic analysis, and beyond. The significance of characteristics in the overall functioning of a Biometric System cannot be understated. The criteria used to assess the suitability of physical or behavioral traits of a human as a biometric modality include universality, uniqueness, permanence, measurability, acceptability, performance, and circumvention.

2 METHOD

2.1 Types of biometric systems are mentioned here.

- **Fingerprint Biometric System:** The fingerprint is one of the most well-known biometric identifiers and has been in use for more than a century due to its uniqueness and durability. Its broad use and long-term collection by immigration and law enforcement, as well as its numerous data collection sources, including the ten fingers, have contributed to its enormous popularity.
- **Hand Geometry Biometric System: This** simple and cost-effective procedure uses a physical inspection to confirm a person's identity. Included are hand size, finger length, breadth, and form. Because to its adaptability, social acceptability, and integration potential, this biometric approach is extensively utilized. Due to its lack of difference, this method's drawback is that it only allows for one-to-one matching. By including new biometric traits, hand recognition accuracy can be increased.
- **Face Recognition System:** People may be identified and characterized by their unique facial structure, which consists of peaks and valleys of varied heights. The biometric system uses this trait to differentiate between people. The face scan records and stores a person's face for future enrolment verification purposes. Simple geometric models gave way to increasingly complex mathematical representations and matching algorithms as face recognition technology advanced.
- **Iris Biometric Recognition System:** One of the most reliable biometric identification and verification techniques recently developed is iris scan technology. The biometric technology system that uses the eye to identify a person is under the eye category. The method of identifying someone based on their iris pattern is known as iris recognition.
- **Hand Written Recognition System:** A person needs a writing instrument in their hand in order to sign using the handwriting and signature technology that has been approved by the government, the legal system, and companies and is utilized by the majority of industries for identification and verification. Using dynamic signature recognition and a person's traits, a location may be determined. To do this, it is necessary to analyze the X, Y, and Z axes' distinctive strokes' speed, velocity, timing, and direction.
- **Voice Recognition Biometric System:** The voice recognition system uses an individual’s voice for determining identity based on the different characteristic voice features. The system for the synthesis of the sound produced by the larynx. The Centre for Laryngeal and Voice Disorder at John Hopkins Hospital described the critical role of the larynx, which is situated in the anterior neck. During the enrollment process using voice recognition technology, a

particular voice for an individual is recorded and stored in a master template and used for further verification of that particular individual.

- **Palmprint Biometrics System:** The technology for palmprint biometric identification is new compared to other biometric identifying methods like face, fingerprint, and iris. The palmprint is recognizable, reliable, and extremely valuable. Similar to fingerprints, palmprints feature delta points, major lines, minute details, wrinkles, and ridges. Nonetheless, it is believed to have precise and unique identifying characteristics since it has a bigger surface area than fingerprints and hand geometry of the biometric data collected by the sensor.

2.2 Stages Involved in a Biometric System during Recognition

Biometric systems undergo a series of crucial steps, including pre-processing to enhance data accuracy, region of interest (ROI) selection for feature extraction influenced by return on investment (ROI), and feature extraction to construct unique data representations. Feature extraction aims to reduce dataset size while preserving essential information. Matching modules compare newly created templates with reference templates, generating match scores to validate claimed identities. Overall, these steps ensure efficient and accurate biometric recognition processes. Figure 2 shows the stages Involved in a Biometric System during Recognition

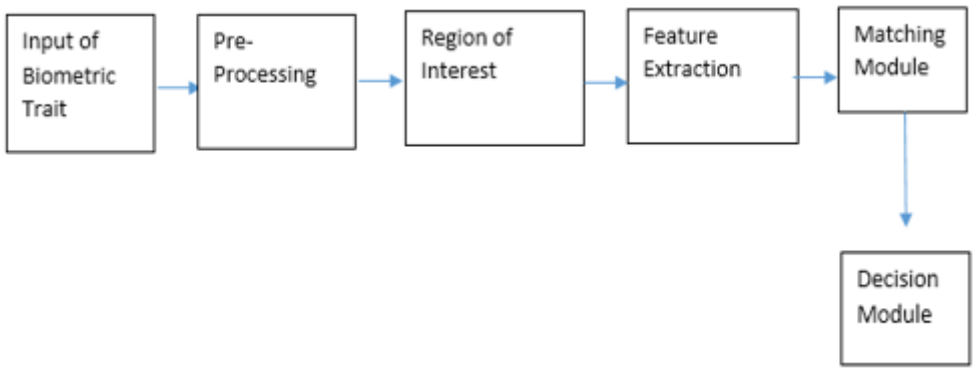

Figure 2 Stages Involved in a Biometric System during Recognition

- **Pre-processing:** The biometric systems pre-processing, feature extraction, matching, and decision-making steps are included. At the pre-processing stage, the computer is employed to enhance the accuracy of the biometric data collected by the sensor.
- **Region of interest stage:** The Region of Interest (ROI) approach is used by biometric systems before to or simultaneously with the feature extraction step. The selection of biometric feature qualities to be used as matching criteria in a biometric system is influenced by return on investment (ROI).
- **Feature Extraction:** The extraction of characteristics is fundamental for recognition systems. The most essential information is taken from the inspected biometric data to construct a new data representation. Everyone’s ideal new representation would be unique. In the identification process for biometric systems, the extraction of characteristics is an essential stage. It involves using less resources to analyses a large volume of data. By removing information that may be used to categorize and acquire visual input patterns, feature extraction's main goal is to lower

the size of the original dataset. For an offline handwritten signing system, static and phony-dynamic feature extraction approaches have been developed.

- **Matching Module:** The newly created template is compared to one or more reference templates by the matching algorithm. The result of the matching algorithm is match score, indicating how similar the templates are. The number of matching between the input template and the stored reference template feature sets is determined and a match score reported. Match scores are used to validate a claimed identity in order to identify an individual. Figure 3 shows the performance of the various biometric sensing systems

Factors	Biometric Sensing Systems									
	Finger print	Face	Hand Geometry	Iris	Voice	Hand Signatory	Gait	Ear	Palm Vein	Palmprint
Accuracy	High	Low	Medium	High	Medium	Medium	High	High	High	High
Ease of Use	High	Medium	High	Medium	High	High	Medium	Medium	Medium	Medium
Cost	Low	Medium	Medium	High	High	Low	High	High	High	High
Privacy	High	High	Medium	High	High	High	High	Low	Low	Medium
Distinctiveness	High	Low	Medium	High	Low	Medium	Medium	High	High	High
Error Causing Factor	Age	Occlusion	Injury	Eye Angle	Illness	Inconsistency	Weight Gain	Pose	Illness	Age
Barrier to Universality	Worn Ridges	Plastic Surgery	Hand Impairment	Visual Impairment	Speech Impairment	Forging	Drunkenness	Lighting Conditions	Ageing	Worn prints

Figure 3 Performance of the various biometric sensing systems

2.2.1 3D on 2D Biometrics

A unique multi-view, multi-spectral 3D finger imaging system is the subject, [14] As far as we currently know, this biometric imaging device seems to be the first of its type that can record a wide variety of information obtained from the finger. A number of fingers' external skin and interior veins were imaged using 3D finger imaging technology. Six different angles were used to scan the fingers in order to accomplish this. To generate 3D finger models with veins and skin textures, the recommended 3D reconstruction and texture mapping techniques are applied. As a benchmark dataset, the Large-scale Finger Multi-Biometric database and benchmark for 3D Finger Biometrics (LFMB-3DFB) is developed. Ten times each of its 695 fingers is captured by the LFMB-3DFB, yielding 83,400 images and 6,950 3D finger models in total. Six skin and six vein images are used to depict each finger. Ultimately, a thorough and methodical evaluation procedure is made in order to carry out in-depth experimental research and analysis on this database. Tasks like subject-independent verification and subject-independent close-set identification are the focus of these investigations and analyses. The best results are obtained

by using extensive and rigorous testing for multi-view finger characteristics recognition, 2D finger traits identification, 3D finger traits recognition, and score-level fusion on LFMB-3DFB.

While 3D finger knuckle detection is an image recognition challenge in and of itself, [15] has demonstrated that substantial variation between the train and test dataset distributions and a lack of training data negatively impact the performance of generic deep neural networks, such as ResNet. These difficulties restrict the ability of generic neural networks to classify authentic identities in a more general way. The advancement of 3D reconstruction techniques has sparked a surge in the exploration of biometric identification through the utilization of 3D data. The utilization of three-dimensional data from finger knuckle patterns offers additional information that is complementary and invariant to illumination [16]. This enhances the reliability and accuracy of biometric identification. The utilization of deep learning techniques has undergone extensive research for a wide range of computer vision applications, including biometrics. The utilization of deep learning techniques was also employed in the cutting-edge development of 3D finger knuckle identification. The proposed method aims to mitigate the issue of uneven finger knuckle patterns by incorporating intermediate information from multiple-scale deep neural networks simultaneously.

The utilization of 3D finger knuckle imaging for identification is strengthened by its greater accuracy, enhanced security, and user-friendly characteristics compared to 2D imaging and other biometric methods. This technology captures intricate details and depth of the knuckle patterns, offering unique biometric signatures that significantly improve recognition performance. The depth information inherent in 3D images ensures robustness against variations in lighting and orientation, and provides a formidable defense against spoofing attempts, making it highly secure. Additionally, the non-intrusive, contactless nature of this technology aligns with a seamless user experience, promoting wider acceptance and application in high-security areas, financial transactions, and secure access controls. Collectively, these benefits justify the adoption of 3D finger knuckle traits as a reliable and efficient method for biometric identification.

2.2.2 Advantages of 3D over 2D Biometric Systems

With the development of the global economy and information technology, particularly with the advent of the Internet era, a growing number of professions now require reliable identity verification. In the context of data, identity is progressively digitized and concealed [17]. Verifying a person's identity and upholding information security are challenging tasks in the digital era. Biometrics are well-known field of research due to its reliability and simplicity of usage. The use of biometric recognition technologies and systems has greatly benefited a number of businesses [18]. Due to its ability to provide identity verification qualities like ease, non-repudiation, and forgery resistance that traditional encryption cannot, biometric identification technology is becoming more and more relevant in people's daily lives. Humans, on the other hand, use "multi-biological feature recognition" to distinguish and identify people based on traits including appearance (facial recognition), speaking style (voice recognition), and stride (gait recognition). The fusion of multibiological feature recognition based on matching scores is determined by the final conclusion, which is generated from the matching

scores of these numerous recognitions [19]. This is crucial to the accuracy of human biometric identification capabilities. So, it is conceivable to assert that multibiological identification based on similarity scores is essential to people's capacity to establish their own identities. So, after demonstrating the essential expertise in recognizing a variety of biological features. Biometric identification authenticates an individual's identity by using their physical or behavioral characteristics. The process of human biometric identification may also be divided into two stages: "registration" and "recognition," whereby the "registration" stage involves storing various biometrics in memory and the "recognition" stage involves recalling and comparing those biometrics.

The state, gesture, and brightness of the image all affect how well face-based biometric face identification algorithms work. Facial image processing-based biometric systems may be impacted by a variety of factors, including the subject's age, the quality of the ambient light, the imaging angle, and the observer's attitude. Biometric data collection, preprocessing, feature extraction, and pattern recognition are the standard four steps in biometric recognition. Although many classification algorithms work well in research settings, there are no conclusions that can be relied upon in situations when time is concerned and there are large databases.

These days, a lot of civic applications make use of biometric systems based on characteristics like the fingerprint, palmprint, face, and iris. Because of the structural characteristics of the hand, which are theoretically singular, time-invariant, and highly exploitable for identification, hand-based biometrics are becoming more and more popular. Applying pressure to the characteristic being scanned in traditional methods for acquiring 2D physiological data results in elastic distortions that have a negative influence on matching accuracy. With contactless image sensing, it is possible to get clear images while also preventing residual imprints. Traditional methods for acquiring contactless 2D images are prone to illumination problems and are open to spoof attempts. Hence the creation of contactless 3D imaging methods for human identification are resistant to light fluctuations, limits problems with skin deformations, and reduce the likelihood of spoof assaults.

2.3 Unimodal Biometric systems

A unimodal (or solitary) biometric system uses a single biometric characteristic [20] or a single information source to confirm or identify a person. Theoretically, unimodal systems have become more accurate and reliable over time, but in practice, registration issues arise because of non-universal biometric characteristics, spoofing, and inaccurate data, as noted above. Fingerprint recognition [21] analyses the distribution of lines on the surface of the finger using a method based on fingerprint recognition to look for certain traits. The vast majority of consumers are open to using fingerprint identification as a type of biometric security, even if a sizeable portion of the general public is used to it. The technology is also functional and accessible. It is important to keep in mind that different fingerprint recognition systems have varying acceptance and rejection error rates. While comparing two faces, a facial recognition system [22] examines how various facial features are arranged. Sometimes, external characteristics like the skin are also considered. Biometric face recognition is possible by face detection technology, which can recognize several faces in pictures. If a remote recognition system is required, recent advancements in this technology make it a great choice for biometric security. Moreover, the technology's capability to "negatively identify" people or remove faces

makes it much easier to spot suspicious people in a crowd. A scanner looks at the distinctive characteristics of the iris during an iris scan [23], which leads in the recording of those characteristics as a (bar) code. Particularly when done with infrared light, iris scanning is recognized as a reliable biometric security technique. Palm vein pattern recognition is based on recognizing unique vein patterns, [24]. While using more reference points than finger vein pattern recognition, this method of identifying is easier and more secure. The most refined biometric security system currently in use uses nonreplicable iris scanning technology (or can only be recreated with great difficulty). A high level of convenience is offered via quick and accurate palm scanning for the user. Moreover, unimodal biometric technologies are less useful than they would be in practical settings. Thus, one solution to these issues is a multimodal biometric identification system. Additional research is needed on the drawbacks of unimodal biometric systems.

- Noisy Data Biometric data occasionally contains noise when sensors are not properly maintained. The most common source of audible fingerprints is dust on the fingerprint scanner sensor. Another form of noisy data is errors in voice output during enrolment. If the camera is not correctly focused, photos of the face and iris may seem blurry.
- Non-Universality biometric system is termed universal when all users can identify themselves using the same biometric feature. Unfortunately, not every biometric feature is distinct. As a result, the system's database cannot include information on these people. Around 2% of the population, including those with disabilities and others who run across numerous roadblocks during a regular registration process, are known to be unable to produce high-quality fingerprints.
- Lack of Individuality Similar features may be gathered using biometric technology, such as a face recognition system that takes pictures of the face. Some situations include father and son or identical twins. More false matches happen because of the uniqueness problem.

  In Biometric system, majority of physiological and behavioral characteristics are distinctive to each individual, identity cards, passwords, and other traditional identifying techniques fall short of biometrics. Several nations, like India, use biometrics to prevent identity theft and maintain national security, incorporating them into security-related procedures. To identify people, several biometric authentication and identification systems combine fingerprints, hands, faces, and signatures. Physiological and behavioral characteristics are used by biometric identification systems to identify people. The algorithm selects biometrics based on each one's unique advantages and disadvantages. Multimodal biometrics more efficiently serve the criteria of the authentication system, even if no one biometric can meet the needs of all applications [25].

  A multimodal ultrasonic recognition system is experimentally evaluated on the basis of the fusion of 3D hand geometry and 3D palmprint data. The technique produces a volumetric image of the complete hand and divides it into several two-dimensional pictures with different depths for each characteristic. The 2D properties of each image are gathered and then appropriately combined in order to create a 3D template. a ground-breaking biometric method using non-contact 3D fingernail scanning. With this method, finger knuckles are simultaneously photographed in 3D and 2D, which allows for a level of precision in matching that may not be possible with only 2D or 3D patterns.

2.4 Multimodal biometric systems

This method integrates the results of several biometric traits identification. A multimodal biometric system employs several biometric modalities to provide a highly precise and secure biometric identification system, in contrast to a unimodal biometric system, which might lead to non-universality [26]. One element that commonly results in inaccuracies is the deterioration of fingerprints. An error or failure in a multimodal biometric system may not have a impact on a person due to the availability of many biometric technology systems. Thus, a multimodal system's potential to lower the non-enrolment rate is one of its main benefits. By standardizing and balancing the geometric mean and hyperbolic tangent, face and voice were brought together. Ross and Jain used linear discriminant based algorithms, the sum rule, and a decision tree to merge face, fingerprint, and hand geometry biometrics. The sum rule outperformed the others, according to the authors' findings. Approaches for integrating speech and facial biometrics [27] looked at multilayer perception, support vector machines, and tree classifiers. A multimodal biometric system is created using ridge-based fingerprint matching and Eigen face matching. The biometric sensor needs to be linked to the proper user interface before the first module, the sensor module, may collect the user's unprocessed biometric data. The raw biometric data that was captured and sent was then utilized to extract characteristics. The biometric data collected using this approach is of adequate quality for further processing. To compare the quality, the attributes are turned into a digital representation and delivered to the matching module.

The fingerprint is one of the most well-known biometric identifiers and has been in use for more than a century due to its uniqueness and durability. Feature extraction using 3D geometry of surface normal vectors, for accurately encoding the curvature information [28]. Feature comparison using similarity function generated from statistical distribution of the encoded feature space, difficult to design complex feature descriptor with finger deformations Its broad use and long-term collection by immigration and law enforcement, as well as its numerous data collection sources, including the ten fingers, have contributed to its enormous popularity. This simple and cost-effective procedure uses a physical inspection to confirm a person's identity. Included are hand size, finger length, breadth, and form. Because to its adaptability, social acceptability, and integration potential, this biometric approach is extensively utilized [29-30]. Due to its lack of difference, this method's drawback is that it only allows for one-to-one matching. By including new biometric traits, hand recognition accuracy can be increased. People may be identified and characterized by their unique facial structure, which consists of peaks and valleys of varied heights. The biometric system uses this trait to differentiate between people. The face scan records and stores a person's face for future enrolment verification purposes. Simple geometric models gave way to increasingly complex mathematical representations and matching algorithms as face recognition technology advanced. One of the most reliable biometric identification and verification techniques recently developed is iris scan technology [31]. The biometric technology system that uses the eye to identify a person is under the eye category. The method of identifying someone based on their iris pattern is known as iris recognition. A person needs a writing instrument in their hand in order to sign using the handwriting and signature technology that has been approved by the government, the legal system, and companies and is utilized by the majority of industries for identification and verification. Using dynamic signature recognition and a person's traits, a location may be

determined. To do this, it is necessary to analyze the X, Y, and Z axes' distinctive strokes' speed, velocity, timing, and direction [32]. The voice recognition system uses an individual's voice for determining identity based on the different characteristic voice features. The system for the synthesis of the sound produced by the larynx. The Centre for Laryngeal and Voice Disorder at John Hopkins Hospital described the critical role of the larynx, which is situated in the anterior neck. During the enrolment process using voice recognition technology, a particular voice for an individual is recorded and stored in a master template and used for further verification of that particular individual. The technology for palmprint biometric identification is new compared to other biometric identifying methods like face, fingerprint, and iris. The palmprint is recognizable, reliable, and extremely valuable. Like fingerprints, palmprints feature delta points, major lines, minute details, wrinkles, and ridges. Nonetheless, it is believed to have precise and unique identifying characteristics since it has a bigger surface area than fingerprints and hand geometry. Contactless 3D images for identification is invariant to the changes of illuminations, poses less problems related to the deformations of the skin and spoof attacks .Image segmentation using deep learning method using Mask R-CNN [33] extracts the discriminative features of finger knuckle, Palm and face from the 3D surface normal vectors by using surface gradient derivatives. Matching approach uses surface key points for estimating the final shifting parameters, which reduces the computational complexity. However difficult to design complex feature descriptor with finger deformations. CNN approach for recognition from deeply learnt multiscale features and alignment model requires a lot of training data.

Biometric sensing systems have become more common, because of its ability to make use of distinctive biological qualities. The government, as well as private and public organizations, may use technology to fight fraud and identity theft. Biometric sensing technology used to be the safest method of identifying and validating people, aims for public safety. Despite this, high-dimensional data with plenty of redundant and uncorrelated characteristics still present computational complexity issues. In order to reduce dimensionality, speed up computations, and increase precision, a subset of pertinent characteristics is chosen. There are both unimodal and multimodal biometric technologies. The 2D or 3D unimodal biometric system goal is to identify people using just one biometric trait. This method falls short and is unable to provide enough recognition accuracy. Data from several biometric traits are included into the multimodal biometric system. It is more secure than a unimodal system and has the ability to get beyond issues like erratic sensor data, lack of universality, uniqueness, and biometric traits.

3 CONCLUSION

In the comparison between 3D and 2D biometric identification technologies, the three-dimensional approach excels in capturing the intrinsic details and in-depth information of biometric traits, offering a more accurate, secure, and reliable means of identification. Its robustness to environmental variations and enhanced anti-spoofing capabilities further solidify its advantage over 2D imaging, which is more susceptible to forgery and less effective under varying conditions. The user-friendly, contactless nature of 3D imaging technology not only improves the user experience but also encourages wider adoption across various security-sensitive applications.

Thus, when it comes to biometric identification, 3D imaging represents a significant advancement over traditional 2D methods, setting a new standard for accuracy, security, and convenience in the Biometrics field.

ACKNOWLEDGEMENT:

I would like to express our sincere gratitude to all those who have supported and contributed to this research project. Primarily, I extend our heartfelt thanks to our guide for her unwavering guidance, invaluable insights, and encouragement throughout the research process. No funding is raised for this research.

REFERENCES

[1] M. Hammad, Y. Liu and K. Wang, "Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint," in IEEE Access, vol. 7, pp. 26527-26542, 2019, doi: 10.1109/ACCESS.2018.2886573.

[2] R. Das, E. Piciucco, E. Maiorana and P. Campisi, "Convolutional Neural Network for Finger-Vein-Based Biometric Identification," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 360-373, Feb. 2019, doi: 10.1109/TIFS.2018.2850320.

[3] A. Tarannum, Z. U. Rahman, L. K. Rao, T. Srinivasulu and A. Lay-Ekuakille, "An Efficient Multi-Modal Biometric Sensing and Authentication Framework for Distributed Applications," in IEEE Sensors Journal, vol. 20, no. 24, pp. 15014-15025, 15 Dec.15, 2020, doi: 10.1109/JSEN.2020.3012536.

[4] Izadeen GY, Ameen SY. Smart android graphical password strategy: A review. Asian Journal of Research in Computer Science. 2021;59-69, DOI: 10.9734/ajrcos/2021/v9i230220.

[5] Premakumari Pujar, Ashutosh Kumar, Vineet Kumar, “Efficient plant leaf detection through machine learning approach based on corn leaf image classification” IAES International Journal of Artificial Intelligence (IJ-AI), Vol. 13, No. 1, March 2024, pp. 1139~1148, ISSN: 2252-8938, DOI: 10.11591/ijai.v13.i1.pp1139-1148.

[6] Sreedhara, S.H., Kumar, V., Salma, S. (2023). Efficient Big Data Clustering Using Adhoc Fuzzy C Means and Auto-Encoder CNN. In: Smys, S., Kamel, K.A., Palanisamy, R. (eds) Inventive Computation and Information Technologies. Lecture Notes in Networks and Systems, vol 563. Springer, Singapore. https://doi.org/10.1007/978-981-19-7402-1_25

[7] Q. Zhang, "Deep Learning of Electrocardiography Dynamics for Biometric Human Identification in era of IoT," 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2018, pp. 885-888, doi: 10.1109/UEMCON.2018.8796676.

[8] K. H. M. Cheng and A. Kumar, "Contactless Biometric Identification Using 3D Finger Knuckle Patterns," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 42, no. 8, pp. 1868-1883, 1 Aug. 2020, doi: 10.1109/TPAMI.2019.2904232.

[9] M. Bassi and P. Triverbi, "Human Biometric Identification through Brain Print," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 1514-1518, doi: 10.1109/ICECA.2018.8474646.

[10] R. S. Kuzu, E. Piciucco, E. Maiorana and P. Campisi, "On-the-Fly Finger-Vein-Based Biometric Recognition Using Deep Neural Networks," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2641-2654, 2020, doi: 10.1109/TIFS.2020.2971144.

[11] Jaswal, G., Kaul, A., Nath, R. (2019). Multimodal Biometric Authentication System Using Hand Shape, Palm Print, and Hand Geometry. In: Verma, N., Ghosh, A. (eds) Computational Intelligence: Theories, Applications and Future Directions - Volume II. Advances in Intelligent Systems and Computing, vol 799. Springer, Singapore. https://doi.org/10.1007/978-981-13-1135-2_42

[12] K. Přihodová and M. Hub, "Biometric Privacy through Hand Geometry- A Survey," 2019 International Conference on Information and Digital Technologies (IDT), Zilina, Slovakia, 2019, pp. 395-401, doi: 10.1109/DT.2019.8813660.

[13] Wang N, Dong J, Fang H, Li B, Zhai K, Ma D, Shen Y, Hu H. 3D reconstruction and segmentation system for pavement potholes based on improved structure-from-motion (SFM) and deep learning. Construction and Building Materials. 2023 Sep 22; 398:132499, doi.org/10.1016/j.conbuildmat.2023.132499.

[14] W. Kang, H. Liu, W. Luo and F. Deng, "Study of a Full-View 3D Finger Vein Verification Technique," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1175-1189, 2020, doi: 10.1109/TIFS.2019.2928507.

[15] D. H. Al-Janabi and A. M. Al-Juboori, "3D-Finger knuckle Recognition using Convolutional Neural Network," *2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCTIT)*, Baghdad, Iraq, 2022, pp. 175-178, doi: 10.1109/CSCTIT56299.2022.10145675.

[16] [1]Chen, S., Guo, Z., Feng, J., and Zhou, J., “An Improved Contact-Based High-Resolution Palmprint Image Acquisition System”, <i>IEEE Transactions on Instrumentation Measurement, vol. 69, no. 9, IEEE, pp. 6816–6827, 2020. doi:10.1109/TIM.2020.2976081.

[17] K. H. M. Cheng and A. Kumar, "Accurate 3D Finger Knuckle Recognition Using Auto-Generated Similarity Functions," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 3, no. 2, pp. 203-213, April 2021, doi: 10.1109/TBIOM.2021.3051062.

[18] D. Palma, P. L. Montessoro, G. Giordano and F. Blanchini, "Biometric Palmprint Verification: A Dynamical System Approach," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 12, pp. 2676-2687, Dec. 2019, doi: 10.1109/TSMC.2017.2771232.

[19] G. Jaswal and R.C. Poonia. Selection of optimized features for fusion of palm print and finger knuckle- based person authentication. Expert Systems, 38(1), p.e12523, 2021, doi.org/10.1111/exsy.12523.

[20] Arora, S., Bhatia, M.P.S., Kukreja, H. (2021). A Multimodal Biometric System for Secure User Identification Based on Deep Learning. In: Yang, XS., Sherratt, R.S., Dey, N., Joshi, A. (eds) Proceedings of Fifth International Congress on Information and Communication Technology. ICICT 2020. Advances in Intelligent Systems and Computing, vol 1183. Springer, Singapore. https://doi.org/10.1007/978-981-15-5856-6_8

[21] M. O. Oloyede and G. P. Hancke, "Unimodal and Multimodal Biometric Sensing Systems: A Review," in IEEE Access, vol. 4, pp. 7532-7555, 2016, doi: 10.1109/ACCESS.2016.2614720.

[22] Yang, B., Xiang, X., Xu, D. et al. 3D palmprint recognition using shape index representation and fragile bits. Multimed Tools Appl 76, 15357–15375 (2017). https://doi.org/10.1007/s11042-016-3832-1

[23] R. S. Kuzu, E. Maiorana and P. Campisi, "Gender-Specific Characteristics for Hand-Vein Biometric Recognition: Analysis and Exploitation," in IEEE Access, vol. 11, pp. 11700-11710, 2023, doi: 10.1109/ACCESS.2023.3239894.

[24] P. Basak, S. De, M. Agarwal, A. Malhotra, M. Vatsa and R. Singh, "Multimodal biometric recognition for toddlers and pre-school children," 2017 IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, USA, 2017, pp. 627-633, doi: 10.1109/BTAS.2017.8272750.

[25] M. S. Lohith, Y. S. K. Manjunath and M. N. Eshwarappa, "Multimodal biometric person authentication using face, ear and periocular region based on convolution neural networks," International Journal of Image and Graphics, vol. 3, pp. 235, 2021, https://doi.org/10.1142/S0219467823500195.

[26] 2017. Stereo-based palmprint recognition in various 3D postures. Expert Syst. Appl. 78, C (July 2017), 74–88. https://doi.org/10.1016/j.eswa.2017.01.025

[27] E. A. Alkeem, C. Y. Yeun, J. Yun, P. D. Yoo, M. Chae et al., "Robust deep identification using ECG and multimodal biometrics for industrial internet of things," Ad Hoc Networks, vol. 121, pp. 102581, 2021, doi.org/10.1016/j.adhoc.2021.102581.

[28] S. Li, B. Zhang, L. Fei, S. Zhao and Y. Zhou, "Learning Sparse and Discriminative Multimodal Feature Codes for Finger Recognition," in IEEE Transactions on Multimedia, vol. 25, pp. 805-815, 2023, doi: 10.1109/TMM.2021.3132166.

[29] S. Li and B. Zhang, "Joint Discriminative Sparse Coding for Robust Hand-Based Multimodal Recognition," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3186-3198, 2021, doi: 10.1109/TIFS.2021.3074315.

[30] K. H. M. Cheng and A. Kumar, "Efficient and Accurate 3D Finger Knuckle Matching Using Surface Key Points," in *IEEE Transactions on Image Processing*, vol. 29, pp. 8903-8915, 2020, doi: 10.1109/TIP.2020.3021294.

[31] K. H. M. Cheng and A. Kumar, "Deep Feature Collaboration for Challenging 3D Finger Knuckle Identification," in *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1158-1173, 2021, doi: 10.1109/TIFS.2020.3029906.

[32] W. Yang, Z. Chen, J. Huang, L. Wang and W. Kang, "LFMB-3DFB: A Large-scale Finger Multi-Biometric Database and Benchmark for 3D Finger Biometrics," *2021 IEEE International Joint Conference on Biometrics (IJCB)*, Shenzhen, China, 2021, pp. 1-8, doi: 10.1109/IJCB52358.2021.9484369.

[33] W. Yang, Z. Chen, J. Huang and W. Kang, "A Novel System and Experimental Study for 3D Finger Multibiometrics," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 4, no. 4, pp. 471-485, Oct. 2022, doi: 10.1109/TBIOM.2022.3181121.