IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 14, No. 4, August 2025, pp. 3143~3152
ISSN: 2252-8938, DOI: 10.11591/ijai.v14.i4.pp3143-3152

Survey on 3D biometric traits for human identification

Divya Gangachannaiah[1], Mamatha Aruvanalli Shivaraj[2], Honganur Chandrasekharaiah Nagaraj[1], Prasanna Gururaj Paga[1]

[1]Department of Electronics and Communication Engineering, Nitte Meenakshi Institute of Technology (NMIT), Nitte (Deemed to be University), Bengaluru, India
[2]Department of Electronics and Communication Engineering, NMAM Institute of Technology (NMAMIT), Nitte (Deemed to be University), Nitte, India

Article Info

Article history:

Received Apr 16, 2024
Revised Feb 22, 2025
Accepted Mar 15, 2025

Keywords:

3D biometric trait
Biometric finger knuckle
Biometric identifier
Finger geometry patterns
Mean square error
Physiological traits

ABSTRACT

Individuals are verified and identified using Biometric technology based on their biological or behavioral traits. Biometric-based personal authentication systems are more reliable and user friendly, overruns the traditional personal authentication systems. The physiological biometric traits get abraded due to aging and massive work, while the behavioral biometric traits are having high variations due to external factors such as fatigue, and mood. 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 traits, 3D reconstruction is done using 2D multiple images. 3D images are usually more robust and illumination invariant as compared to their 2D counterparts. 3D reconstruction algorithms are compared by finding mean square error (MSE).

Corresponding Author:

Mamatha Aruvanalli Shivaraj
Associate Professor, Department of Electronics and Communication Engineering
NMAM Institute of Technology, Nitte (Deemed to be University)
Nitte, Karnataka, India
Email: mamathag__12@rediffmail.com

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 personal identification numbers (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 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 have 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.

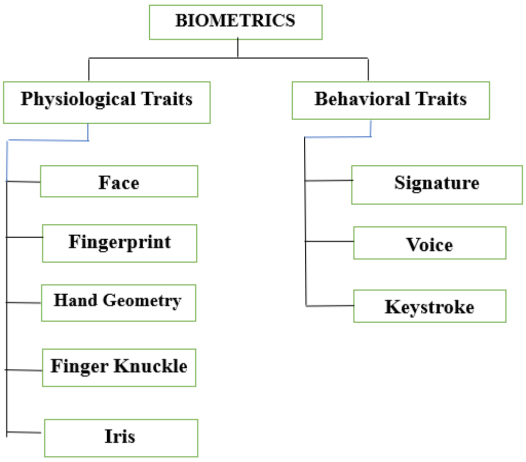

Figure 1. Biometric classification

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 shifts 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].

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

Using distinctive physiological or behavioral characteristics, such as fingerprints, facial features, iris patterns, or voice characteristics, biometric identification is a multi-step process that confirms a person's identity. The procedure starts with enrollment, in which specialized sensors are used to collect biometric data, which is then transformed into a digital template and safely stored in a database. The technology gathers fresh biometric information from the person during identification and analyzes it to obtain unique characteristics. Advanced matching techniques are then used to compare this processed data with the templates that have been stored.

2.1. Types of biometric systems are mentioned here

Biometric identification systems have become increasingly important in enhancing security and ensuring accurate personal authentication in various domains. These systems utilize an individual's unique physiological and behavioral traits, thus providing a reliable and efficient alternative to traditional identification methods such as passwords or identity cards. As technology advances, various biometric modalities have been developed-each with different features, benefits, and limitations-offering a wide array of solutions tailored to specific application needs. Some commonly used types of biometric systems include:

- 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.
- 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.zed. 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. 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.
- 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.

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 selection for feature extraction influenced by return on investment, 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.

- 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 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.
- 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.

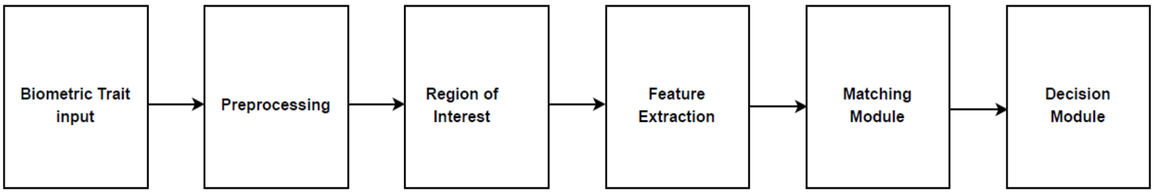

Figure 2. Stages involved in a biometric system during recognition

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. While 3D finger knuckle detection is an image recognition challenge in and of itself, Al-Janabi and Al-Juboori [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.

2.2.2. 3D reconstruction

3D reconstruction of biometric traits is an advanced technique that involves creating three-dimensional models of human biometric features for recognition, authentication, and analysis. This technology enhances security, accuracy, and robustness in biometric systems. 3D fingerprint models capture ridge depth and skin elasticity, offering better resistance to spoofing attacks. 3D reconstruction is being done using Frankot-Chellappa (FC) algorithm and Poisson solver (PO) algorithm [17]. The FC algorithm is used for integrating a gradient field into a surface by ensuring integrability using Fourier transforms. A PO is often used to solve the 2D or 3D Poisson equation and is commonly employed in scenarios like shape-from-shading or seamless image cloning. 2D multiple input forefinger finger knuckle images of subject 1 [18] considering six input multiple images of finger knuckle print, out of 192 subjects with each seven images of forefinger and seven images of middle finger. Figure 3 shows the output 3D reconstructed image obtained from FC algorithm which gives more depth information efficiently. In comparison with Figure 4, depth information is distributed above the reference which implicates normalization is not effective and images are blurred near the edges using PO method.

In 3D image processing and analysis, statistical parameters play a crucial role in characterizing, evaluating, and interpreting volumetric data. These parameters assist in quantifying surface textures, assessing algorithm performance, and modeling complex structures. Figure 5 gives an overview of mean square error (MSE) plot, which is widely used metric for evaluating the accuracy of 3D image processing algorithms. It quantifies the average squared difference between corresponding elements of two 3D datasets, typically a reconstructed image and its ground truth.

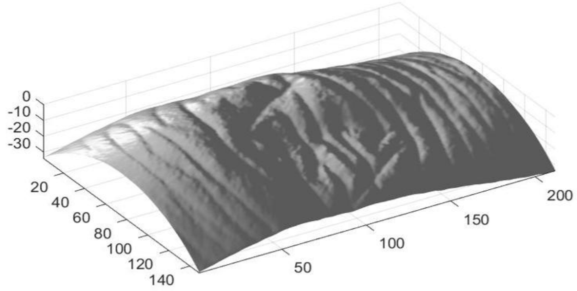

Figure 3. 3D image from FC algorithm

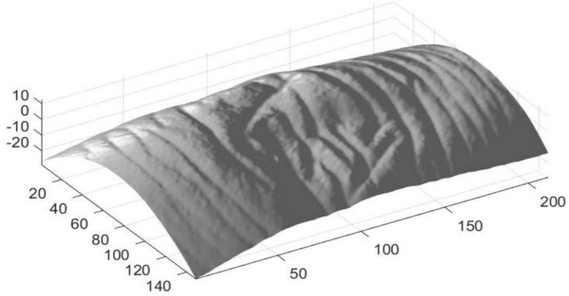

Figure 4. 3D image from poison solver algorithm

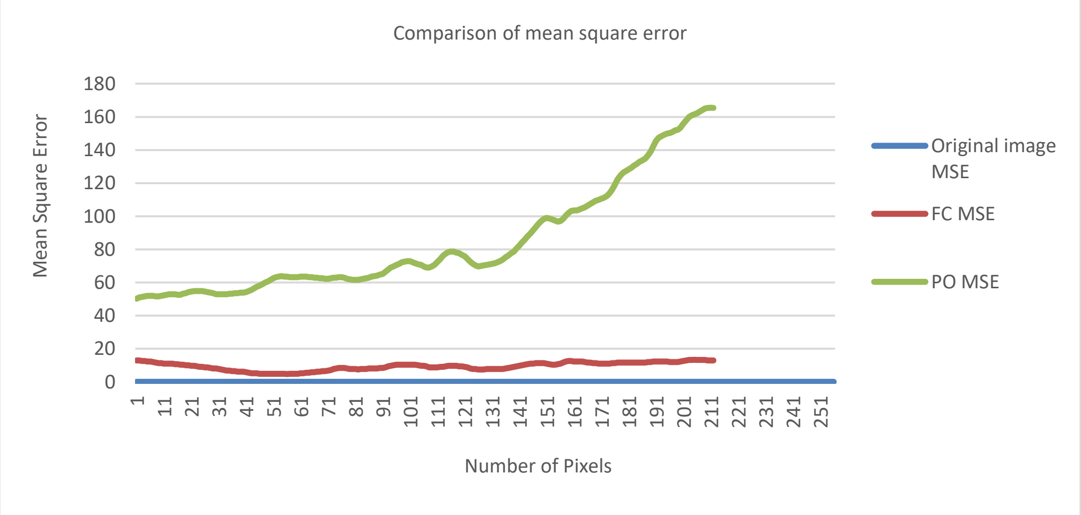

Figure 5. MSE comparison between FC and Poisson

2.2.3. 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 [19]. 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 [20]. 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 [21]. 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. 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 [22] 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 [23] 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 [24] 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 [25], 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 [26]. While using more reference points than finger vein pattern recognition, this method of identifying is easier and more secure. Adaptive linear interpolation algorithm is used for 3D reconstruction [27], which uses triangulation method. 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.
- Non-universality biometric system is termed universal when all users can identify themselves using the same biometric feature. 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.

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 [28]. One element that commonly results in inaccuracies is the deterioration of fingerprints. An error or failure in a multimodal biometric system may not have an 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 [29] 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 [30]. 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 [31], [32]. 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 [17]. 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 [22]. Contactless 3D images for identification are 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 [34].

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. 3D reconstruction algorithms are being analyzed by finding MSE. MSE is close to zero in FC algorithm compared to PO algorithm. 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

We would like to express our heartfelt thanks to our guide for her unwavering guidance, invaluable insights, and encouragement throughout the research process. We would also like to thank Nitte Meenakshi Institute of Technology for providing the necessary support for carrying out this research.

FUNDING INFORMATION

The authors would like to inform that this project has been funded by the Karnataka State Council for Science and Technology (KSCST) Bangalore.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration. The authors would like to inform that the team consisted of four members, each of whom contributed meaningfully to the overall development of the paper. The detailed rubrics used for the analysis are enclosed herein.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Divya Gangachannaiah	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Mamatha Aruvanalli Shivaraj	✓	✓			✓	✓			✓	✓	✓	✓		✓
Honganur Chandrasekharaiah Nagaraj	✓	✓			✓	✓			✓	✓	✓	✓		✓
Prasanna Gururaj Paga		✓							✓	✓	✓			

C :	**C**onceptualization	I :	**I**nvestigation	Vi :	**Vi**sualization
M :	**M**ethodology	R :	**R**esources	Su :	**Su**pervision
So :	**So**ftware	D :	**D**ata Curation	P :	**P**roject administration
Va :	**Va**lidation	O :	Writing - **O**riginal Draft	Fu :	**Fu**nding acquisition
Fo :	**Fo**rmal analysis	E :	Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

The authors would like to declare that there is no conflict of interest pertaining to financial, personal, or professional in connection with the manuscripts.

INFORMED CONSENT

The authors would like to inform that the data sets have been taken with prior consent from Hong Kong Polytechnic university.

DATA AVAILABILITY

The authors would like to inform that the data set for carrying out the research is publicly available in https://www4.comp.polyu.edu.hk/~csajaykr/3DKnuckle.htm. Official consent for using the database was obtained from the Hong Kong Polytechnic university.

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,” *IEEE Access*, vol. 7, pp. 25527–25542, 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,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 360–373, Feb. 2018, 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,” *IEEE Sensors Journal*, vol. 20, no. 24, pp. 15014–15025, 2020, doi: 10.1109/JSEN.2020.3012536.

[4] G. Y. Izadeen and S. Y. Ameen, “Smart android graphical password strategy: a review,” *Asian Journal of Research in Computer Science*, pp. 59–69, 2021, doi: 10.9734/ajrcos/2021/v9i230220.

[5] P. Pujar, A. Kumar, and V. Kumar, “Plant leaf detection through machine learning based image classification approach,” *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 13, no. 1, pp. 1139–1148, Mar. 2024, doi: 10.11591/ijai.v13.i1.pp1139-1148.

[6] S. H. Sreedhara, V. Kumar, and S. Salma, “Efficient big data clustering using adhoc fuzzy c means and auto-encoder CNN,” *Lecture Notes in Networks and Systems*, vol. 563, pp. 353–368, 2023, doi: 10.1007/978-981-19-7402-1_25.

[7] Q. Zhang, “Deep learning of electrocardiography dynamics for biometric human identification in era of IoT,” in *2018 9th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2018*, 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,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 42, no. 8, pp. 1868–1883, 2020, doi: 10.1109/TPAMI.2019.2904232.

[9] M. Bassi and P. Triverbi, “Human biometric identification through brain print,” in *Proceedings of the 2nd International Conference on Electronics, Communication and Aerospace Technology, ICECA 2018*, 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,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2641–2654, 2020, doi: 10.1109/TIFS.2020.2971144.

[11] G. Jaswal, A. Kaul, and R. Nath, “Multimodal biometric authentication system using hand shape, palm print, and hand geometry,” *Advances in Intelligent Systems and Computing*, vol. 799, pp. 557–570, 2019, doi: 10.1007/978-981-13-1135-2_42.

[12] K. Prihodova and M. Hub, “Biometric privacy through hand geometry-a survey,” in *Proceedings of the International Conference on Information and Digital Technologies 2019, IDT 2019*, 2019, pp. 395–401, doi: 10.1109/DT.2019.8813660.

[13] N. Wang *et al.*, “3D reconstruction and segmentation system for pavement potholes based on improved structure-from-motion (SFM) and deep learning,” *Construction and Building Materials*, vol. 398, 2023, doi: 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,” *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,” in *Proceedings - CSCTIT 2022: 5th College of Science International Conference on Recent Trends in Information Technology*, 2022, pp. 175–178, doi: 10.1109/CSCTIT56299.2022.10145675.

[16] S. Chen, Z. Guo, J. Feng, and J. Zhou, “An improved contact-based high-resolution palmprint image acquisition system,” *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 9, pp. 6816–6827, 2020, doi: 10.1109/TIM.2020.2976081.

[17] K. H. M. Cheng and A. Kumar, “Efficient and accurate 3D finger knuckle matching using surface key points,” *IEEE Transactions on Image Processing*, vol. 29, pp. 8903–8915, 2020, doi: 10.1109/TIP.2020.3021294.

[18] A. Kumar, “The Hong Kong Polytechnic University contactless 3D finger KnuckleImages database,” *The Hong Kong Polytechnic University*, 2019. [Online]. Available: https://www4.comp.polyu.edu.hk/~csajaykr/3DKnuckle.htm

[19] K. H. M. Cheng and A. Kumar, “Accurate 3D finger knuckle recognition using auto-generated similarity functions,” *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 2, pp. 203–213, 2021, doi: 10.1109/TBIOM.2021.3051062.

[20] D. Palma, P. L. Montessoro, G. Giordano, and F. Blanchini, “Biometric palmprint verification: a dynamical system approach,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 12, pp. 2676–2687, 2019, doi: 10.1109/TSMC.2017.2771232.

[21] G. Jaswal and R. C. Poonia, “Selection of optimized features for fusion of palm print and finger knuckle-based person authentication,” *Expert Systems*, vol. 38, no. 1, 2021, doi: 10.1111/exsy.12523.

[22] K. H. M. Cheng and A. Kumar, “Deep feature collaboration for challenging 3D finger knuckle identification,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1158–1173, 2021, doi: 10.1109/TIFS.2020.3029906.

[23] S. Arora, M. P. S. Bhatia, and H. Kukreja, “A multimodal biometric system for secure user identification based on deep learning,” *Proceedings of Fifth International Congress on Information and Communication Technology (ICICT 2020)*, Oct. 2020, pp. 95–103, doi: 10.1007/978-981-15-5856-6_8.

[24] M. O. Oloyede and G. P. Hancke, “Unimodal and multimodal biometric sensing systems: a review,” *IEEE Access*, vol. 4, pp. 7532–7555, 2016, doi: 10.1109/ACCESS.2016.2614720.

[25] B. Yang, X. Xiang, D. Xu, X. Wang, and X. Yang, “3D palmprint recognition using shape index representation and fragile bits,” *Multimedia Tools and Applications*, vol. 76, no. 14, pp. 15357–15375, 2017, doi: 10.1007/s11042-016-3832-1.

[26] R. S. Kuzu, E. Maiorana, and P. Campisi, “Gender-specific characteristics for hand-vein biometric recognition: analysis and exploitation,” *IEEE Access*, vol. 11, pp. 11700–11710, 2023, doi: 10.1109/ACCESS.2023.3239894.

[27] G. Divya, G. P. Prasanna, M. Madhushree, A. Achut, and Vishwa, “Adaptive linear interpolation algorithm for 2D DICOM multiple skull images,” in *2024 5th IEEE Global Conference for Advancement in Technology (GCAT)*, Oct. 2024, vol. 11, no. 1, pp. 1–5, doi: 10.1109/GCAT62922.2024.10924040.

[28] 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. 23, no. 2, 2023, doi: 10.1142/S0219467823500195.

[29] Ö. Bingöl and M. Ekinci, “Stereo-based palmprint recognition in various 3D postures,” *Expert Systems with Applications*, vol. 78, pp. 74–88, 2017, doi: 10.1016/j.eswa.2017.01.025.

[30] E. Al Alkeem *et al.*, “Robust deep identification using ECG and multimodal biometrics for industrial internet of things,” *Ad Hoc Networks*, vol. 121, 2021, doi: 10.1016/j.adhoc.2021.102581.

[31] S. Li, B. Zhang, L. Fei, S. Zhao, and Y. Zhou, “Learning sparse and discriminative multimodal feature codes for finger recognition,” *IEEE Transactions on Multimedia*, vol. 25, pp. 805–815, 2023, doi: 10.1109/TMM.2021.3132166.

[32] S. Li and B. Zhang, “Joint discriminative sparse coding for robust hand-based multimodal recognition,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3186–3198, 2021, doi: 10.1109/TIFS.2021.3074315.

[33] 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, doi: 10.1109/IJCB52358.2021.9484369.

[34] W. Yang, Z. Chen, J. Huang, and W. Kang, “A novel system and experimental study for 3D finger multibiometrics,” *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 4, no. 4, pp. 471–485, 2022, doi: 10.1109/TBIOM.2022.3181121.

BIOGRAPHIES OF AUTHORS

Divya Gangachannaiah is currently working as an Assistant Professor Grad III in Electronics and Communication Engineering of Nitte Meenakshi Institute of Technology, Yelahanka, and Bangalore. She completed her B.E. in Electronics and Communication Engineering from East Point College of Engineering and Technology Bangalore and M.Tech. in Digital Electronics from East West Institute of Technology Bangalore. She has 17 years of teaching experience. Presently pursing her Ph.D. in Nitte University Mangalore. Her areas of interest are signal processing and image processing. She can be contacted at email: divyag_12@rediffmail.com.

Mamatha Aruvanalli Shivaraj is currently working as Associate Professor in the Department of Electronics and Communication Engineering at NMAM Institute of Technology, Nitte, Udupi, Karnataka, India. She has 25 years of teaching experience. She is the author of nine international journals and six international conferences in the field of multispectral image compression. She is the author of the ‘Network theory’, ‘Engineering statistics and linear algebra’, and ‘Control engineering’. Her areas of interest are signal processing, image compression, and control engineering. She is a senior member of IEEE. She can be contacted at email: mamathag_12@rediffmail.com.

Honganur Chandrasekharaiah Nagaraj is currently working as the Principal of NMIT, Bangalore. He holds B.E. (Electronics and Communications) degree from the University of Mysore, M.E. (Communication Systems) degree from P.S.G College of Technology, Coimbatore and Ph.D. (Biomedical Signal Processing and Instrumentation) from Indian Institute of Technology, Chennai. He has teaching experience of almost 4 decades, his aims to bring NMIT among the top 50 education institutes according to NIRF ranking. He has massive experience of 42 years in teaching. He has visited 15 countries and studied the University Engineering Education System, involving various laboratories, and centers of excellence. He has published 80 papers nationally and internationally. He can be contacted at email: principal@nmit.ac.in.

Prasanna Gururaj Paga is currently working as an Associate Professor in Department of Electronics and Communication Engineering at Nitte Meenakshi Institute of Technology, Yelahanka, Bangalore. He completed his B.E. in Electronics and Communication Engineering from PDA College of Engineering Gulbarga and M.Tech. in Industrial Electronics from SJCE Mysore and Ph.D. from University of Mysore on Antennas. He has over 20 publications in reputed journals and conferences. He has over 16 years of teaching experience. He can be contacted at email: prasanna.paga@nmit.ac.in.