PALMPRINT SPOOFING DETECTION USING DEEP LEARNING APPROACH BY USING HYPERSPECTRAL AND MULTISPECTRAL DATA

Abstract

This research work focuses on enhancing the security of palmprint authentication systems by developing an anti-spoofing strategy using deep learning approaches with hyperspectral and multispectral data. We uses printed palmprint and non-imaging palmprint databases, employing CNN, SVM, KNN, and random forest algorithms for classification. The proposed strategy achieves promising identification accuracies of 96.2% (CNN) and 89% (SVM) for spoofing detection. The combined approach reaches an 86% accuracy. The non-imaging database achieves a 70.65% accuracy with KNN and an 84% overall score with random forest. The study highlights the vulnerabilities of biometric systems and proposes effective anti-spoofing measures for palmprint authentication, contributing to enhanced reliability and security. Further research is suggested to improve performance and real-world applicability.

Keywords: Biometric, Hyperspectral, Multispectral, Palmprint, Spoffing.

Authors

Snehal S. Datwase
Department of Computer Science and Information Technology
Dr. Babasaheb Ambedkar Marathwada University
Aurangabad, India.
snehaldatwase@gmail.com

Ratnadeep R. Deshmukh
Department of Computer Science and Information Technology
Dr. Babasaheb Ambedkar MrathwadaUniversity
Aurangabad, India.
rrdeshmukh.csit@bamu.ac.in

I. INTRODUCTION

In today's digitalized world, ensuring the security of information has become a pressing concern for individuals and organizations [1]. To address this issue, verifying the identity of individuals attempting to access systems has become crucial, leading researchers to explore various authentication techniques, such as knowledge-based or token-based methods [2]. While these traditional approaches enhance security, they also have limitations that can be overcome by utilizing biometric technology, which relies on intrinsic characteristics of individuals [3].

Biometrics involves the use of physiological or behavioral traits, such as fingerprints, facial features, iris patterns, speech, and hand shape, to identify individuals [4]. Selecting the appropriate biometric modality is essential when designing a biometric system, as it impacts the success rate of feature extraction [4]. Behavioral traits, while widely accepted, tend to have lower precision due to greater variation among individuals [5]. In contrast, physiological characteristics strike a balance between acceptance and precision rates, with some features offering higher acceptance rates but lower accuracy, like face modalities.

Among various physiological features, the biometric modalities derived from the human hand, such as palmprints and palm-vein patterns, have shown to be reliable and accepted in diverse security applications [6]. Advancements in multispectral imaging now allow capturing both palmprint and palm-vein images using a single acquisition device, with visible light for palmprints and near-infrared (NIR) for palm-veins [7].

While multispectral imaging has been widely studied, recent research has shown increased interest in hyperspectral imaging for biometrics, including face and palmprint recognition [8-13]. Hyperspectral imaging offers a wealth of discriminative information as it provides extensive wavelength coverage and precise resolution [15]. It overcomes limitations of traditional algorithms used in palmprint recognition and effectively addresses various challenges [13, 14].

Hyperspectral imaging in biometrics involves capturing and processing images in dozens of spectral bands, offering a more comprehensive representation of spectral information [16]. In hyperspectral remote sensing, this imaging technique extracts information from the Earth's surface using radiance measured by aerial or space-based sensors across contiguous small spectral bands in the visible and solar reflective infrared spectrum.

The high spectral resolution of hyperspectral imaging provides redundant and unique information about objects or scenes [15]. This technology is being applied to non-imaging palmprint databases, using tools like the ASD Field Spec 4 Spectroradiometer to obtain unique spectral signatures of individuals. More complex palm structures generate more spectral information, enhancing the optical complexity revealed by the palm print's spectrum.

1. **Biometric Authentication:** Biometric authentication has emerged as a highly effective and reliable method for verifying an individual's identity. In our increasingly automated world, accurate identification of individuals plays a crucial role in various tasks, and biometrics offer a promising solution to this challenge. Unlike traditional authentication

methods relying on passwords or possession of items, biometrics leverage unique physical or behavioral characteristics, such as fingerprints, facial features, or voice, to establish a person's identity with a high level of certainty.

In the realm of computer science, biometrics involves measuring and analyzing various aspects of the human body to create distinct individual profiles. For a trait to be considered suitable for biometric authentication, it should possess key properties like universality (present in every individual), uniqueness (no two individuals sharing the same trait), permanence (unchanged over a person's lifetime), and collectability (feasibility of data collection). Other important factors in biometric systems include performance, acceptability, and the level of circumvention difficulty for unauthorized access.

The biometric authentication process involves three main stages: data capture through sensors, feature extraction to create individual datasets, and matching the extracted features against a system database to determine identity similarity.

Despite its potential, biometric technology faces challenges such as spoofing and fraud, necessitating continuous research and improvements. One potential avenue for enhancing biometric systems is through the incorporation of spectroscopy techniques, which may further strengthen the reliability and security of biometric authentication. As technology advances, biometrics continue to pave the way for a future of secure and seamless personal identification.

2. **Types of Biometrics:** Biometrics encompasses various types of unique physical or behavioral characteristics used for authentication. Some common types of biometrics include:

- **Fingerprint:** Analyzing the unique patterns of ridges and valleys on a person's fingertip.
- **Facial Recognition:** Identifying individuals based on distinct facial features, such as the distance between eyes or the shape of the nose.
- **Iris Recognition:** Examining the colored part of the eye to create a unique identifier.
- **Retina Recognition:** Analyzing the unique pattern of blood vessels at the back of the eye.
- **Voice Recognition**: Identifying individuals based on their voice patterns and characteristics.
- **Hand Geometry**: Measuring the size and shape of the hand and fingers.
- **Signature Recognition:** Analyzing the unique style and characteristics of a person's signature.
- **Behavioral Biometrics:** Assessing patterns in behavior, such as keystroke dynamics or gait analysis.

Each of these biometric types offers distinct advantages and limitations, making them suitable for various authentication scenarios.

3. Biometric Models

- **Enhancing Security through Unique Identifiers:** In an era where digital technologies have become pervasive, ensuring robust security measures is of utmost importance. Biometric models have emerged as a cutting-edge solution to enhance security through unique identifiers. These models rely on distinct physiological or behavioural characteristics of individuals, providing reliable and accurate identification and authentication processes. This short paper explores the concept of biometric models, their significance in various applications, and their potential impact on security and privacy.

- **Biometric Models: Defining the Technology:** Biometric models utilize biometric data, which comprises measurable and unique attributes of individuals. These attributes can be broadly categorized into two main types: physiological (related to the body) and behavioral (related to actions). Common physiological biometric identifiers include fingerprint, iris, face, palm, and DNA. Behavioral biometric identifiers encompass signatures, voice patterns, keystroke dynamics, and gait recognition.

- **Importance in Security and Authentication:** Biometric models provide a higher level of security compared to traditional password-based or token-based authentication methods. Unlike passwords, which can be forgotten or stolen, biometric data is difficult to replicate or fake. This makes it significantly more challenging for unauthorized individuals to gain access to secure systems or sensitive data. Biometric models also offer convenience, as users do not need to remember passwords or carry physical tokens for authentication.

- **Applications of Biometric Models:** Biometric models find applications in various domains, ranging from personal devices to national security initiatives. They are commonly used in mobile phones, laptops, and tablets to unlock devices or authorize digital transactions. In law enforcement, biometric models play a crucial role in identifying suspects through fingerprint databases. Governments also employ these models for immigration and border control to ensure enhanced security and prevent identity fraud.

- **Challenges and Concerns:** While biometric models offer several advantages, they are not without challenges and concerns. The collection and storage of biometric data raise privacy issues, and its misuse can lead to severe consequences for individuals. Ensuring the security of biometric databases is paramount, as any breach could compromise the identity of millions. Additionally, there are concerns about the permanence and changeability of biometric identifiers, as certain attributes may alter over time due to injury, aging, or other factors.

4. Performance Evaluation of Biometric Systems: Biometric system performance evaluation assesses the accuracy, efficiency, and reliability of biometric identification and authentication technologies. Metrics such as False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and Receiver Operating Characteristic (ROC) curve are commonly used to measure system effectiveness. Evaluations ensure optimal system configuration, address vulnerabilities, and enhance overall security and user experience.

5. **Application of Biometric Systems:** Biometric systems find widespread applications in various domains, providing secure and efficient identification and authentication solutions. Key applications include:

   - **Access Control:** Biometric systems are used to regulate access to physical locations, such as office buildings, data centers, and restricted areas. Fingerprint, face, and iris recognition ensure only authorized individuals can enter.
   - **Mobile Devices:** Biometric authentication, like fingerprint or facial recognition, is prevalent in smart phones and tablets. It enables quick and secure unlocking of devices and authorizes mobile payments.
   - **Law Enforcement:** Biometric models aid law enforcement agencies in identifying suspects through fingerprint databases and facial recognition systems, aiding investigations.
   - **Border Control and Immigration:** Biometrics are employed at international borders to verify travelers' identities, enhance security, and prevent identity fraud.
   - **Time and Attendance Management:** Biometric systems streamline employee attendance tracking, ensuring accurate records and reducing time theft.
   - **Financial Services:** Biometrics are used in banking and financial institutions for secure customer authentication during transactions and account access.
   - **Healthcare:** Biometric solutions ensure accurate patient identification, reducing medical errors and enhancing data privacy.
   - **Elections:** Biometrics can be used for voter authentication, preventing voter fraud and ensuring fair elections.
   - **Surveillance and Security:** Biometric-based surveillance systems aid in monitoring public spaces and identifying potential threats.
   - **Personal Devices:** Beyond mobile phones, biometric systems are integrated into laptops, tablets, and smart home devices for personalized security.

   These applications showcase the versatility and potential impact of biometric systems in enhancing security and efficiency across various sectors

II. LITERATURE REVIEW

1. **Palmprint Recognition Using Spectroscopic Imaging:** While traditional biometric technologies like fingerprint, voice, iris, and face recognition have limitations in security and usability, palmprint recognition has emerged as an alternative solution. However, capturing high-quality palmprint data remains a challenge, especially with conventional white light sources leading to poor image quality and reduced recognition accuracy. To overcome these limitations and enhance anti-spoofing mechanisms, hyperspectral and multispectral imaging techniques are being employed. Multispectral imaging with red, green, blue, and near-infrared bands offers moderate security, while hyperspectral imaging provides a more detailed and comprehensive dataset by capturing continuous spectral bands. These advancements contribute to the improvement of spectroscopic

Palmprint identification systems, ensuring higher accuracy and efficiency in human authentication. [17]

2. **Multispectral Image:** A multispectral image is a type of digital image that captures information from multiple discrete bands of the electromagnetic spectrum. Unlike traditional RGB (Red, Green, Blue) images, multispectral images encompass a broader range of wavelengths, revealing specific features and characteristics of the observed scene. These images find extensive use in various fields, such as remote sensing, agriculture, environmental monitoring, and medical imaging, enabling advanced analysis and enhanced understanding of the subject matter.

3. **Spectroscopy in Biometric Recognition:** The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

4. **Skin Morphology:** The human skin, the body's largest organ, serves crucial functions of sensation, protection, and regulation. It acts as a protective barrier against UV radiation, water loss, and injuries while regulating body temperature and metabolism. Skin appendages include hair, sebaceous glands, blood vessels, and nerves. The skin has three main layers: the epidermis (outermost), dermis (middle), and hypodermis (innermost). The epidermis consists of multiple layers of cells, with the keratinocyte being the predominant cell type. The dermis contains tissues like mast cells, fibroblasts, blood vessels, collagen, and elastin. The hypodermis is composed mainly of adipose tissue, providing insulation and energy reserves.

5. **Review**

Table 1: Literature Survey on Palmprint

Paper Title	Authors	Methodology	Results
Comparative analysis of palm print recognition system with Repeated Line Tracking method[18]	shashi Balaa et al.	Maximum Curvature approach, Repeated Line Tracking, CLAHE, Log Gabor filter	100% matching score achieved
Palmprint recognition system based on proposed features extraction and (c5.0) decision tree, k-nearest neighbour (knn) classification approaches[19]	Mustafa S. Kadhm1 et al.	Direction, Local Binary Pattern (LBP) features, C5.0, K-Nearest Neighbour (KNN)	99.7% recognition rate, 0.009% error rate
Multispectral Palmprint Encoding and	Zohaib Khan et al.	Contour Code, automatic region of	Error rates of 0.003% on

Recognition[20]		interest extraction, PolyU, CASIA databases	PolyU, 0.2% on CASIA
Research on Palmprint Identification Method Based on Quantum Algorithms[21]	Hui Li et al.	Quantum adaptive median filtering, Quantum Fourier transform, Quantum set operations	Matching accuracy nearly 100%
Band Selection for Palmprint Recognition [22]	Junwen Sun et al.	Band selection on PolyU hyperspectral palmprint database	EER 0.17325%
Analysis of Multibiometric Palmprint Recognition System for Authentication [23]	Akila P et al.	Comparison of left and right palmprint samples, weighted fusion approach	Error rate of 0.06% to 0.2%
Discriminative Local Feature for Hyperspectral Hand Biometrics by Adjusting Image Acutance [24]	Wei Nie et al.	Image acutance modification, Gaussian filters, HDHV and HPV databases	Improved recognition than original images
Palmprint Recognition Based on Phase Congruency and Two-Dimensional Principal Component Analysis [25]	Jinyu Guo et al.	Phase congruency combined with 2DPCA, Recognition rate of 99.44%	Best performance compared to other techniques
Design of Online Non-contact Palmprint Recognition Simulation System[26]	Sen Lin et al.	Non-contact palmprint identification, Recognition rate of 97.48%	Simple, feasible, and successful system
Multi-Feature Fusion Using Collaborative Residual for Hyperspectral Palmprint Recognition [27]	Shuping Zhao et al.	Feature extraction using LBP, LDP, DCNN, Fusion using collaborative residual	EER of 0.11%, Accuracy of 99.76%
Comparative Analysis of Image Enhancement Technique for Hyperspectral Palmprint Images [28]	Anita G. Khandizod et al.	Image enhancement techniques, PolyU Hyperspectral palmprint database	2D median filter yielded the best results
Hyperspectral Palmprint Recognition System using Phase Congurency and KNN Classifier [29]	Anita Gautam Khandizod et al.	Phase congruency, KNN classifier, Recognition accuracy of 95.31%	Effective palmprint recognition
Palmprint Recognition using Rank Level Fusion [30]	Ajay Kumar et al.	Rank level combination for palmprint matchers, Multiple fusion approaches	Improved performance from combination

Multispectral Palmprint Recognition Using a Quaternion Matrix [31]	Xingpeng Xu et al.	Quaternion model for multispectral biometrics, Recognition accuracy of 98.83%	Suitable for real-world applications
Efficient Deep Palmprint Recognition via Distilled Hashing Coding [32]	Huikai Shao et al.	Distilled hashing coding, Deep hashing network, Recognition accuracy of 97.49%	Knowledge distillation improved performance
Palmprint Recognition Using Siamese Network [33]	Dexing Zhong et al.	Siamese network for palmprint recognition, EER of 0.2819%	Efficient palmprint identification
Machine Learning Algorithms based Palmprint Biometric Identification[34]	Midhuna Naveen et al.	Deep learning methodology, RFCNN, Accuracy of 98.36%	RFCN outperformed other algorithms

III. METHODOLOGY AND RESULT

1. Experiment on Multispectral Imaging Database and Spoof Database.

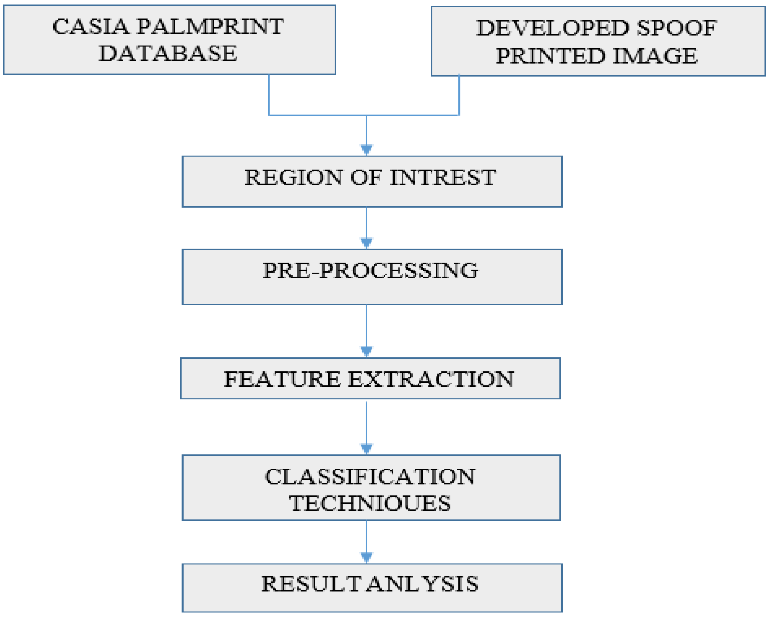

Figure 1: Proposed Methodology for Multispectral Palmprint Database

1. **Multispectral Palmprint Database:** This study utilized the multispectral palmprint database from CASIA University, consisting of 7200 grayscale images captured with an 8-bit JPEG format. Each individual provided six samples captured under six lighting conditions in two separate sessions. Preprocessing steps involved resizing, extracting the Region of Interest (ROI), applying a threshold, and refining the palm region. This resulted in accurate ROI images for further analysis.

2. **Palmprint Spoof Database:** To create a palmprint spoof database, 500 printed copies of palmprint images were generated from the CASIA database (250 left and 250 right palm images). These printed images were scanned using an HP Scanjet 200 scanner and then enhanced using Gaussian and median filters, along with thresholding techniques, to obtain the ideal palmprint's ROI. This ensured that the spoof images closely resembled genuine palmprints.

- **Pre-Processing**

  - Multispectral image
  - Crop and Normalize.
  - Gaussian filter, Median filter.
  - Image Enhancement.

- **Features Extraction & Matching Techniques**

  - Threshold the image.
  - Hough transform.
  - SIFT

- **Classification Technique**

  - **Convolutional Neural Network (CNN):**CNN is a powerful deep learning algorithm widely used in computer vision tasks, including image recognition and classification. It consists of multiple layers of convolutions, pooling, and fully connected layers that automatically learn hierarchical patterns and features from input images. CNNs have shown remarkable success in various image-related tasks, making them a popular choice for palmprint recognition and spoofing detection [35].

  - **Support Vector Machine (SVM):**SVM is a popular supervised machine learning algorithm used for classification and regression tasks. It works by finding an optimal hyperplane that best separates different classes in the feature space. SVM is known for its ability to handle high-dimensional data and is often used for binary classification problems, including palmprint verification and spoofing detection [36].

- **Result:** In this study, we have utilized the CASIA Multispectral Palmprint Database to develop a palmprint recognition system and spoofing detection mechanism. The database contained 7200 grayscale images captured under various lighting conditions using a CCD camera. Preprocessing steps were applied to extract the Region of Interest (ROI) for analysis.To create a spoof database, we have printed 500 copies of the palmprint images and then scanned them using an HP scanner. Various filters and preprocessing techniques were applied to refine the spoof images.For the experimental results, we used a multispectral palmprint database with 500 palmprint reflectance spectra from 25 individuals. We applied image enhancement techniques and evaluated the quality using Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The median filter showed the best results in enhancing image quality.

A Convolutional Neural Network (CNN) was trained for palmprint categorization using triplet loss to improve embeddings. The model achieved a high accuracy of 96.2% in palmprint recognition using CNN and demonstrated an 86% accuracy in detecting spoof images.

The study highlighted the effectiveness of deep learning techniques in palmprint analysis and spoofing detection, contributing to the advancement of biometric authentication systems.

2. Experiment on hyperspectral non-imaging Database

- **Database:** At Dr. Babasaheb Ambedkar Marathwada University, a spectral palmprint database was created using RS3 software in their multispectral research laboratory. The database includes 25 individuals aged between 20 and 50 years. Palmprint reflectance spectra were captured with an 8-degree field of view, obtaining 10 spectral signatures for each participant's left and right palms. In total, the database contains 500 palmprint reflectance spectra, spanning from 350 nm to 2500 nm.

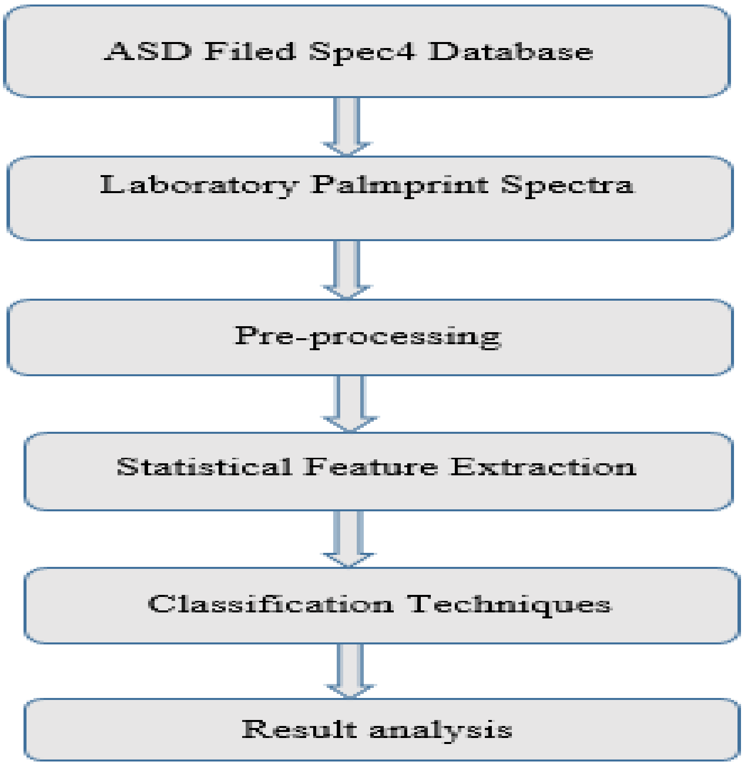
ASD Filed Spec4 Database
Laboratory Palmprint Spectra
Pre-processing
Statistical Feature Extraction
Classification Techniques
Result analysis

Figure 2: Proposed Methodology for hyperspectral database.

- **Classification Techniques:** Random Forest: Random Forest is an ensemble learning algorithm that combines multiple decision trees to improve prediction accuracy and reduce overfitting. Each decision tree is trained on a different subset of the data and features, and the final prediction is made by aggregating the results of individual trees. Random Forest is robust, handles large datasets well, and is commonly used for classification tasks, including palmprint identification and anti-spoofing [37].

  K-Nearest Neighbors (KNN): KNN is a simple and intuitive machine learning algorithm used for classification and regression tasks. In KNN, the class of a new data point is determined based on the majority class of its K nearest neighbors in the feature space. KNN is non-parametric and does not make any assumptions about the underlying data distribution. It is commonly used in palmprint recognition and anti-spoofing tasks [38].

- **Result:** In this work we have created our own hyperspectral non-imaging palmprint database using the ASD Field Spec4 device. The database contained wavelength data ranging from 350 nm to 2500 nm and consisted of 500 samples with left and right palm labels.We split the database into two halves, with 60% used for training their proposed model. The model used logistic regression and K-Nearest Neighbors (KNN) classifiers for classification. The KNN classifiers achieved an accuracy of 70.65%.

  We also employed the random forest technique for further classification and achieved an overall accuracy of 84%. The model's performance was evaluated using precision, recall, and the F1 score.The experimental results demonstrate the potential of palmprint recognition in non-imaging scenarios and highlight the effectiveness of different classification techniques. However, further research and improvement are needed to enhance accuracy and reliability in non-imaging palmprint identification.

IV. CONCLUSION

The research work focuses on developing an anti-spoofing strategy for palmprint authentication using deep learning approaches with hyperspectral and multispectral data. The study utilizes printed palmprint and non-imaging palmprint databases, achieving high accuracy rates of 96.2% (CNN) and 89% (SVM) for spoofing detection. The combined approach reaches an 86% accuracy. The non-imaging database achieves a 70.65% accuracy with KNN and an 84% overall score with random forest. The research underscores the importance of robust anti-spoofing measures in biometric verification systems.

REFERENCES

[1] L. Wang, “Some issues of biometrics: technology intelligence, progressand challenges”, International Journal of Information Technology andManagement, Inderscience publisher, Vol. 11, No. 1/2, pp. 72-72, (2012).

[2] Swanirbhar Majumder, Kharibam Jilenkumari Devi, Subir Kumar Sarkar,“Singular value decomposition and wavelet-based iris biometric watermarking”, IET Biometrics, Vol. 2, Issue 1 , pp. 21-27, (2013)

[3] H. D. Supreetha Gowda, G. Hemantha Kumar & Mohammad Imran,“Multi-modal biometric system on various levels of fusion using LPQfeatures”, Journal of Information and Optimization Sciences, Vol. 39,Issue 1, pp. 169–181, (2018).

[4] Abdallah Meraoumia, Hakim Bendjenna, Salim Chitroub, “Towards arobust palmprint representation for person identification”, InternationalJournal of Information and Communication Technology, Vol.14, No.1,pp. 89-109, (2019).

[5] Khaled Bensid, Djamel Samai, Fatima Zohra Laallam, Abdelah Meraoumia, “Deep learning feature extraction for multispectral palmprintidentification”, J. Electron. Imaging 27(3), 033018 (2018).

[6] Michal Dvorak, Martin Drahansky, “Hand shape recognition and palmprint recognition using 2D and 3D features”, Hand-Based Biometrics:Methods and Technology, pp. 283-307, (2018)

[7] Vartak, P.P., Bharadi, V.A.: ‘Hyperspectral face recognition by texture feature extraction using hybrid wavelets type I & II and kekre wavelet transform’. 2015 Int. Conf. on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2015, pp. 721–727

[8] Ghasemzadeh, A., Demirel, H.: ‘3D discrete wavelet transform based feature extraction for hyperspectral face recognition’, IET Biometrics, 2017, 7, (1), pp. 49–55Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[9] Hong, D., Liu, W., Su, J., et al.: ‘A novel hierarchical approach for multispectral palmprint recognition’, Neurocomputing, 2015, 151, pp. 511– 521

[10] Guo, Z.H., Zhang, L., Zhang, D.: ‘Feature band selection for multispectral palmprint recognition’. 2010 20th Int. Conf. on Pattern Recognition, Istanbul, Turkey, 2010

[11] Li, M., Xie, W., Shen, L.: ‘Fusing 3D gabor and block-wise spatial features for hyperspectral palmprint recognition’. Chinese Conf. on Biometric Recognition, Springer, Cham, 2017, pp. 361–369

[12] G, Z.H., Zhang, D., Zhang, L., et al.: ‘Empirical study of light source selection for palmprint recognition’, Pattern Recognit. Lett., 2011, 32, (2), PP. pp. 120–126

[13] Shen, L., Dai, Z., Jia, S., et al.: ‘Band selection for Gabor feature based hyperspectral palmprint recognition’, 2015 Int. Conf. on Biometrics (ICB), Phuket, Thailand, 2015, pp. 416–421.

[14] Khandizod, A.G., Deshmukh, R.R.: ‘Hyperspectral palmprint recognition: a review’. Int. Conf. on Recent Trends and Challenges in Science and Technology, Ahmednagar, India, 2014

[15] Khandizod, A.G, Deshmukh, R.R.: ‘Comparative analysis of image enhancement technique for hyperspectral palmprint images’, Int. J. Comput. Appl., 2015, 121, pp. 30–35

[16] Shen, L., Dai, Z., Jia, S., et al.: ‘Band selection for Gabor feature based hyperspectral palmprint recognition’, 2015 Int. Conf. on Biometrics (ICB), Phuket, Thailand, 2015, pp. 416–421

[17] P. Tome and S. Marcel, "On the vulnerability of palm vein recognition to spoofing attacks". International Conference on Biometrics (ICB), Phuket, pp. 319-325. doi: 10.1109/ICB.2015.7139056, 2015.

[18] Bala, Shashi. "Comparative analysis of palm print recognition system with Repeated Line Tracking method." Procedia Computer Science 92 (2016): 578-582.

[19] Kadhm, Mustafa S., Hayder Ayad, and Mamoun Jassim Mohammed. "PALMPRINT RECOGNITION SYSTEM BASED ON PROPOSED FEATURES EXTRACTION AND (C5. 0) DECISION TREE, K-NEAREST NEIGHBOUR (KNN) CLASSIFICATION APPROACHES." Journal of Engineering Science and Technology 16.1 (2021): 816-831.

[20] Khan, Zohaib, et al. "Multispectral palmprint encoding and recognition." arXiv preprint arXiv:1402.2941 (2014).

[21] Li, Hui, and Zhanzhan Zhang. "Research on palmprint identification method based on quantum algorithms." The Scientific World Journal 2014 (2014).

[22] Guo, Zhenhua, et al. "Feature band selection for online multispectral palmprint recognition." IEEE Transactions on Information Forensics and Security 7.3 (2012): 1094-1099.

[23] Bhaskar, Bhagya, and S. Veluchamy. "Hand based multibiometric authentication using local feature extraction." 2014 International Conference on Recent Trends in Information Technology. IEEE, 2014.

[24] Nie, Wei, Bob Zhang, and Shuping Zhao. "Discriminative local feature for hyperspectral hand biometrics by adjusting image acutance." Applied Sciences 9.19 (2019): 4178.

[25] Guo, Jinyu, Yuqin Liu, and Weiqi Yuan. "Palmprint recognition based on phase congruency and two-dimensional principal component analysis." 2011 4th International Congress on Image and Signal Processing. Vol. 3. IEEE, 2011.

[26] Lin, Sen, Yuchen Bai, and Yonghua Tang. "Design of online non-contact palmprint recognition simulation system." 2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI). IEEE, 2016.

[27] Zhao, Shuping, Wei Nie, and Bob Zhang. "Multi-feature fusion using collaborative residual for hyperspectral palmprint recognition." 2018 IEEE 4th International Conference on Computer and Communications (ICCC). IEEE, 2018.

[28] Khandizod, Anita G., and R. R. Deshmukh. "Comparative analysis of image enhancement technique for hyperspectral palmprint images." International Journal of Computer Applications 121.23 (2015): 30-35.

[29] Khandizod, Anita & Deshmukh, Ratnadeep. (2018). Hyperspectral Palmprint Recognition System using Phase Congurency and KNN Classifier.

[30] Kumar, Ajay, and Sumit Shekhar. "Palmprint recognition using rank level fusion." 2010 IEEE International Conference on Image Processing. IEEE, 2010.

[31] Xu, Xingpeng, et al. "Multispectral palmprint recognition using a quaternion matrix." Sensors 12.4 (2012): 4633-4647.

[32] Shao, Huikai, Dexing Zhong, and Xuefeng Du. "Efficient deep palmprint recognition via distilled hashing coding." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. 2019.

[33] Zhong, Dexing, Yuan Yang, and Xuefeng Du. "Palmprint recognition using siamese network." Chinese conference on biometric recognition. Springer, Cham, 2018.

[34] Naveen, Midhuna, et al. "Machine Learning Algorithms based Palmprint Biometric Identification."

[35] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.)

[36] Cortes, C., & Vapnik, V. (1995). Support-vector networks. Machine learning, 20(3), 273-297.)

[37] Breiman, L. (2001). Random forests. Machine learning, 45(1), 5-32.)

[38] Cover, T. M., & Hart, P. E. (1967). Nearest neighbor pattern classification. IEEE transactions on information theory, 13(1), 21-27.)