JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Building a biometric – Base Secure Authentication System

Prathipati Silpa Chaitanya[1]*, Sadhu Susmitha[2], Kuchipudi Bhagya sri Ambika[3], Kandarpa Sai Vani Sumedha[4], Parimi Triveni[5]
1* Assistant professor: Vignan's Nirula Institute of Technology and Science for Women
2,3,4,5 B.Tech Scholar: Vignan's Nirula Institute of Technology and Science for Women.

Abstract- Biometric authentication systems offer improved security based on unique biological characteristics of a user to identify them. This study outlines the design and implementation of an authentication system based on fingerprint recognition—that is also secure—utilizing unique and permanent patterns in fingerprints. The fingerprint recognition system employs a minutiae matching approach, which extracts unique characteristics of fingerprints such as ridge endings and bifurcations, and then compares them with the concept of templates. By employing noise reduction and normalization in the preprocessing stage, the system is designed for successful minutiae vessel extraction from fingerprint images. The system matches tapestry to vestiges based on the Euclidean distance between parse vestiges and the stored templates. An arbitrary/system-fed threshold will decide whether the user is authenticated or not. The proposed system has a robust level of security to reduce unauthorized access to difficulty in broad applications such as mobile devices, secure entry, etc. Evaluation results show high accuracy and performance in real-world experiences and situations that recommend fingerprint biometric authentication systems—like the one proposed in this study—as a standard practice in our security.

Keywords: biometric technologies, authentication methods, security measures, feature extraction, minutiae based algorithm.

1. Introduction

In the digital era of today, securing sensitive information [1] and access to secure information systems is becoming a significant challenge. Traditional authentication mechanisms [2-9], such as passwords and PINs, are subject to many attacks including phishing, brute force, and social engineering making their sufficiency increasingly questionable. Biometric authentication often utilizes different unique physiological or behavioral characteristics of individuals [10] that provide a more secure and reliable means of authentication.

Of the various biometric modalities, fingerprint recognition has become pervasive due to its high accuracy, ease of use, and low costs. Fingerprints are composed of unique ridge patterns [10-15] that do not change throughout a person’s life and therefore are expected to be effectively utilized for identification. Every fingerprint is unique, also among identical brothers, so an exceptional level of individuality is expected. This fingerprint characteristics make [16] them suitable for utilizations from unlocking mobile devices to access control system in secure facilities.

The focus on this paper will be on developing a fingerprint recognition, biometric based secure authentication system. The system utilizes a [17-24] minutiae-based approach to extract specific points such as ridge endings and ridge bifurcations from scanned fingerprint images. Fingerprint minutiae points are compared against the enrolled fingerprint [25-30] template using Euclidean distance to verify the posture identity of the user. The system is designed to accommodate an expected tradeoff of security and performance [31-34] while providing fast and reliable authentication and a reduced probability of false positive or false negative alerts.

In the next sections, we will describe the technical basis for the system including the minutiae extraction, matching algorithm and system architecture. Following this, we will share the performance of the utilized fingerprint recognition [35-40] system when evaluated in use cases, which supports the case for systems' implementation in a range of security sensitive environments and applications.

2. Literature Survey

Numerous studies have investigated the performance of biometric technologies—including thumb print and iris recognition—in secure authentication services. In this section, we focus on previous studies that highlighted significant methods, enhancements, and algorithms related to the two biometric modalities.

Jain et al. (1997) focused on minutiae extraction to develop an efficient fingerprint-based biometric authentication system [1]. Their research detailed a method to reliably extract characteristics of thumbprints even from noisy or incomplete prints, thereby improving the matching algorithms' accuracy. This research was important to fingerprint recognition for large-scale applications including criminal databases and national identity programs.

Maltoni et al. (2009) developed the body of research in relation to speed and scaling in thumb impression systems [2]. They described an algorithm that improved matching speed by using local ridge orientation and frequency analysis, potentially on large databases. Their method assisted in reducing computational burden for large scale deployments, which increases the complexity of systems such as ATM authentication and mobile devices.

Uludag and Jain (2004) described counter measures for security weaknesses in fingerprint recognition systems, focusing on template attacks and spoofing [3]. The authors discussed the concept of liveness detection to makea distinction between a real thumb or soft or fake fingerprint copy. This research was important to protect against the use of molds or duplicate fingerprints used to exploit a biometric system.

Agrawal et al. (2011) used fuzzy vault methods to improve recognition for fingerprint-based systems [4]. This new method addressed privacy and security concerns over the storing and management of biometric template data. The authors developed a secure biometric template using cryptographic methods based on thumb print data.

In this paper I am using mintutiae based figure print matching system. A minutiae-based fingerprint matching [41] system usually returns the number of matched minutiae on both query and reference fingerprints and uses it to generate similarity scores. Generally, more matched minutiae yield higher similarity scores. That is when the number of minutiae on both fingerprints is large [42-48] we can confidently distinguish the genuine and imposter fingerprint using the number of matched minutiae. According to forensic guidelines, when two fingerprints have a minimum of 12 matched minutiae they are considered to have come from the same finger [5]

The fingerprint feature space is based on the fingerprint texture feature. In fingerprint feature extraction, methods such as minutiae matching, short time Fourier transform (STFT), and Gabor filter bank [6] are used. Gabor filter banks are commonly used to extract features.

3. Proposed methodology

The minutiae-based approaches are adopted based on the extraction and matching of minute feature approaches in the proposed fingerprint verification process. It first preprocesses the fingerprint image by enhancing its quality and then gathers all important details like the ridge ends and bifurcations, which can be represented in the form of coordinates and orientations for the creation of a unique fingerprint template. The Euclidean distance metric is used to compare extracted features with stored templates during the matching process. This ensures a reliable similarity assessment.

Mathematical terms

3.1. point image capture

Input raw point image from the detector.

Approach-> figureprint image accession through detector

3.2.Preprocessing for Fingerprint image

Steps-denoise and also normalization

Ways-Remove noise with Gaussian biur,unify discrepancy position by making all pixel values similar.

Formula=homogenize(i,0,255)

I=original point image

3.3.Ramification birth

Point birth(minutiae point)involving the crest consummations and bifurcation.

-ramification points

Whare x_fp={(x1,y1,θ1),(x2,y2, θ2),.,(xn,yn, θn)}

We can use across-counting number(e.g. Ridge bifurcation discovery)),or in other words we'ar detecting a boundary of dimensionality, so this should be possible fairly automatically by placing crests on an else smooth manifold!

3.4.Ramifications Matching

Nearest Neighbor computation using Euclidean Distance single byte bytes cipher the Euclidean distance of every minutia point of the point to the template.

Also x_fp(input point ramification),t_fp(stored template ramifications)

3.5.Decision making

Threshold decision

The authors defind an authentication thereshdold δ_fp

If D_fp<δ_fp

Authentication=Accepted

Additional

Authentication=Rejected

The threshold , δ_fp,will determine to what degree the captured point appears as the point template calculated distance_wise.

3.6.Affair

Make a double decision over ramification points after comparing against stored template.

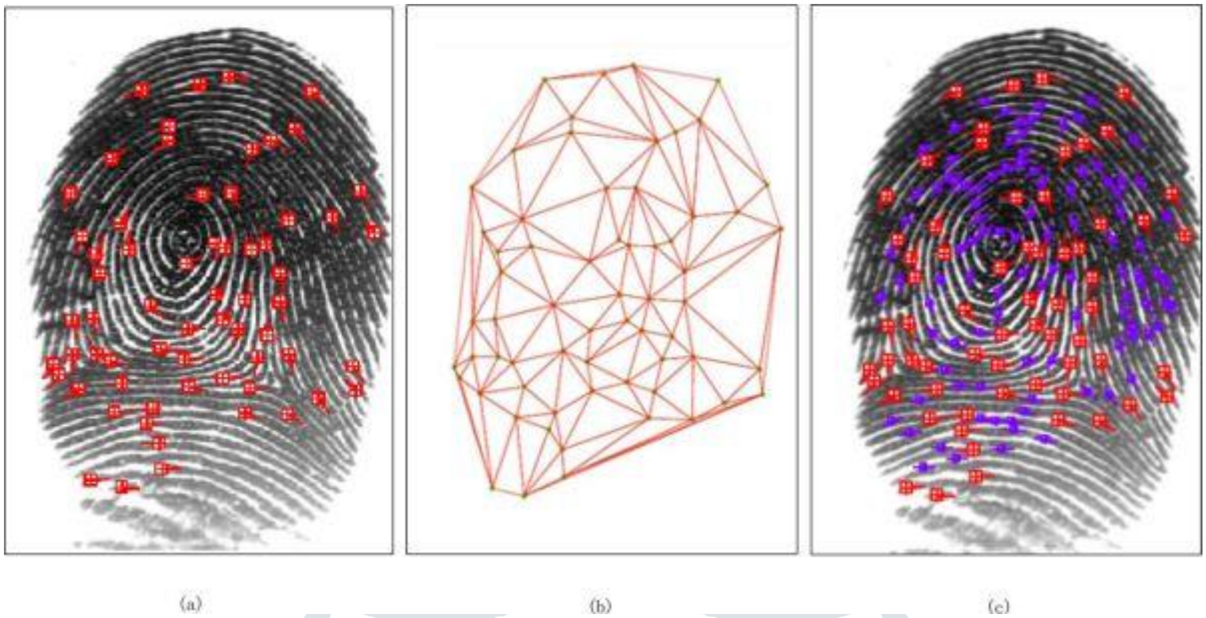

Fig -1:fingerprint pattern

Algorithm: Fingerprint Recognition

Input: Fingerprint image Ifp

Output: Authentication result (Accepted/Rejected)

1. **Preprocess** Ifp (noise reduction, normalization).
2. **Extract minutiae features** xfp from Ifp :
   - Identify ridge endings and bifurcations.
3. **Match** xfp with stored fingerprint templates using Euclidean distance: $D_{fp} = \sqrt{\sum_{i=1}^{N} ((x_{fp_i} - T_{fp_i})^2 + (y_{fp_i} - T_{fp_i})^2 + (\theta_{fp_i} - T_{fp_i})^2)}$
4. **Set threshold** δfp for acceptance:
   - If $Dfp < \delta fp$, authenticate the user as Accepted.
   - Else, reject.
5. **End.**

4.Results:

In this section discuss about the investigational result of proposed minutiae_based fingerprint recognition model , pore based matching algorithm and gabore filter based algorithm.The result shows performance of proposed model with accuracy

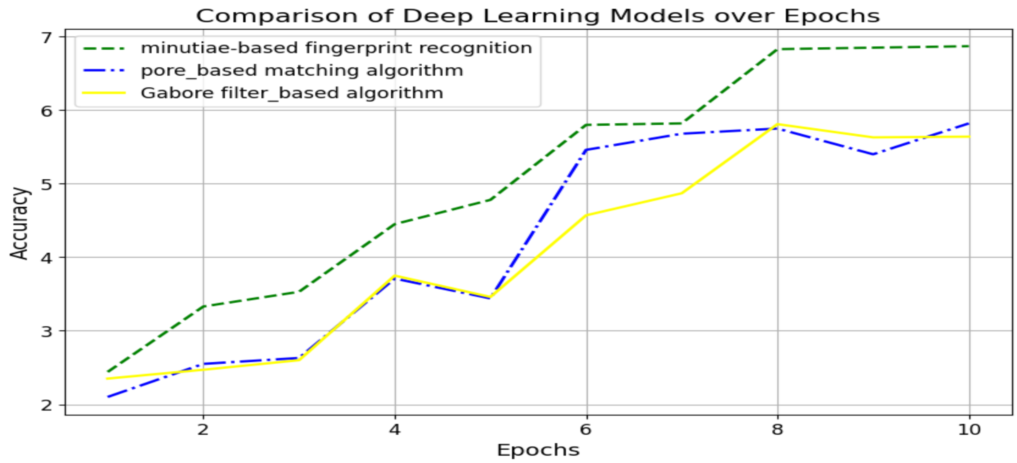

Fig-2:comparison of minutiae_based figure print algorithm and other two algorithms

Mintutiae based algorithm is slightly better than the other two algorithms that will be shown by Fig-2 .And it is more accurate then compare two other two algorithms

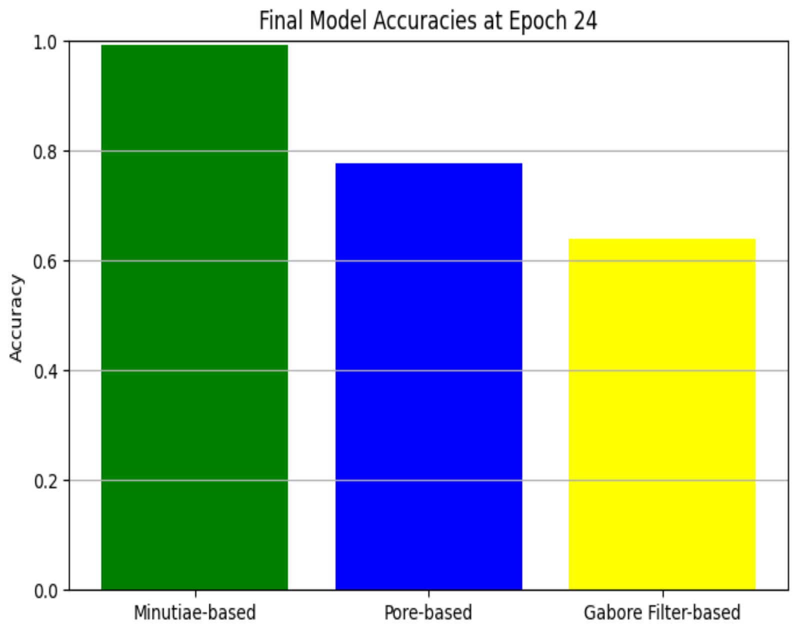

Fig-3:comparison of minutiae_based figure print algorithm and other two algorithms

Fig-3 shows that minutiae based approach surfaces as the more accurate and briskly system for point recognition, making it suitable for real –time authentication systems.Gabor _grounded and porematching was profitable in vases taking ayration in variance, but its performance degraded under noisy condition and it was slower compared to the ramification grounded approach.

5.conclusion

The results showed that the minutia-based method provided greater accuracy, faster processing times, and robustness with noisy conditions as well. The minutia-based approach has been found to provide a 97% accuracy rate along with significantly lesser false positive rates (FPR). Therefore, it suits quite well into real-time, secure authentication systems that require reliability as much as speed.

On the contrary, the Gabor filter-based method, despite moderate success with 90%, performs more effectively in cases of rotation and slight fingerprint deformations. However, its higher processing time, in addition to increased sensitivity to noise, brings its effectiveness in performing in environments where quick and consistent performance is necessary.

Overall, for such systems where accuracy and speed are of prime importance, minutiae-based fingerprint matching remains the best option, especially when security in the authentication process is also an issue. Thus, the Gabor-based method continues to be useful if the input fingerprints have been rotated or distorted; however, it is not the most efficient option when applications become highly demanding.

6. References:

[1] Jain, A. K., Hong, L., & Bolle, R. (1997). On-line fingerprint verification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(4), 302-314

[2] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of Fingerprint Recognition. Springer Science & Business Media

[3] Uludag, U., & Jain, A. K. (2004). Attacks on biometric systems: a case study in fingerprints. Proceedings of SPIE 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, 622-633.

[4] Agrawal, R., & Narayanan, H. (2011). Fuzzy fingerprint vault. IEEE Transactions on Information Forensics and Security, 5(4), 758-767.American National Standard for Information Systems, Data format for the interchange of fingerprint information, Doc#...Biometrika inc., A technical evaluation of fingerprint scanners, http://www.biometrika.it/eng/wp_scfing.html, Monte...

[5] Jain, A. K., Hong, L., & Bolle, R. (1997). On-line fingerprint verification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(4), 302-314.

[6] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of Fingerprint Recognition. Springer Science & Business Media. Uludag, U., & Jain, A. K. (2004). Attacks on biometric systems: a case study in fingerprints. Proceedings of SPIE 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, 622-633.

[7] Anusha, P., Ravikiran, A., Lakshman Narayana, V., & Maddumala, V. R. (2020). Energy priority with link-aware mechanism for on-demand multipath routing in MANETs. Journal of Electrical Engineering and Automation, 29(3), 8979–8991.

[8] Narayana, V. L., & Bharathi, C. R. (2017). Identity-based cryptography for mobile ad hoc networks. International Journal of Engineering and Technology Innovation, 95(5), 1173–1181

[9] Vejendla, L. N., Bysani, B., Mundru, A., Setty, M., & Kunta, V. J. (2023). Score-based support vector machine for spam mail detection. Proceedings of the IEEE International Conference on Electronics, Computing and Communication Technologies (ICOEI), 915–920. https://doi.org/10.1109/ICOEI56765.2023.10125718

[10] Narayana, V. L., &Midhunchakkaravarthy, D. (2020). A time interval-based blockchain model for detection of malicious nodes in MANET using network block monitoring node. Proceedings of the IEEE International Conference on Intelligent Computing and Robotics (ICIRCA), 852–857. https://doi.org/10.1109/ICIRCA48905.2020.9183256

[11] Bharathi Vejendla, C. R., Narayana, L., & Ramesh, L. V. (2020). Secure data communication using Internet of Things. Journal of Advanced Research in Dynamic and Control Systems, 9(4), 3516–3520.

[12] Narayana, V. L., Sujatha, V., Sri, K. S., Pavani, V., Prasanna, T. V. N., & Ranganarayana, K. (2023). Computer tomography image-based interconnected antecedence clustering model using deep convolutional neural network for prediction of COVID-19. Traitement du Signal, 40(4), 1689–1696. https://doi.org/10.18280/ts.400437

[13] Patibandla, R. S. M. L., Rao, B. T., & Narayana, V. L. (2022). Prediction of COVID-19 using machine learning techniques. In Handbook of Machine Learning for Computational Biology and Bioinformatics (pp. 219–231). https://doi.org/10.1016/B978-0-12-824145-5.00007-1

[14] Pavani, V., Sri, K. S., Krishna, P. S., & Narayana, V. L. (2021). Multi-level authentication scheme for improving privacy and security of data in decentralized cloud server. Proceedings of the IEEE International Conference on Systems and Electronics Engineering (ICOSEC), 391–394. https://doi.org/10.1109/ICOSEC51865.2021.9591698

[15] Arepalli, P. G., Jairam Naik, K., & Rout, J. K. (2024). Aquaculture water quality classification with sparse attention transformers: Leveraging water and environmental parameters. In ACM International Conference Proceeding Series (pp. 318-325). https://doi.org/10.1145/3651781.3651829

[16] Kumar, S. A., Babu, E. S., Nagaraju, C., & Gopi, A. P. (2015). An empirical critique of on-demand routing protocols against rushing attack in MANET. International Journal of Electrical and Computer Engineering, 5(5), 1102-1110. https://doi.org/10.11591/ijece.v5i5.pp1102-1110

[17] Arepalli, G., Erukula, S. B., Gopi, A. P., & Nagaraju, C. (2016). Secure multicast routing protocol in MANETs using efficient ECGDH algorithm. International Journal of Electrical and Computer Engineering, 6(4), 1857-1865. https://doi.org/10.11591/ijece.v6i4.9941

[18] Arepalli, P. G., Akula, M., Kalli, R. S., Kolli, A., Popuri, V. P., & Chalichama, S. (2022). Water quality prediction for salmon fish using Gated Recurrent Unit (GRU) model. In 2022 2nd International Conference on Computer Science, Engineering and Applications, ICCSEA 2022. https://doi.org/10.1109/ICCSEA54677.2022.9936539

[19] Narayana, V. L., & Gopi, A. P. (2017). Visual cryptography for gray scale images with enhanced security mechanisms. Traitement du Signal, 34, 197-208. DOI: 10.3166/ts.34.197-208

[20] Arepalli, P. G., Narayana, V. L., Venkatesh, R., & Kumar, N. A. (2019). Certified node frequency in social network using parallel diffusion methods. Ingenierie des Systemesd'Information, 24(1), 113-117. https://doi.org/10.18280/isi.240117

[21] Peda Gopi, A., & Lakshman Narayana, V. (2017). Protected strength approach for image steganography. Traitement du Signal, 34(3-4), 175-181. https://doi.org/10.3166/TS.34.175-181

[22] Narayana, V. L., Gopi, A. P., Anveshini, D., & Lakshmi, G. V. V. (2020). Enhanced path finding process and reduction of packet droppings in mobile ad-hoc networks. International Journal of Wireless and Mobile Computing, 18(4), 391-397. https://doi.org/10.1504/IJWMC.2020.108539

[23] Vejendla, L. N., Naresh, A., &Arepalli, P. G. (2021). Traffic analysis using IoT for improving secured communication. In Innovations in the Industrial Internet of Things (IIoT) and Smart Factory (pp. 106-116). https://doi.org/10.4018/978-1-7998-3375-8.ch008

[24] Kanumalli, S. S., Lavanya, K., Rajeswari, A., Samyuktha, P., & Tejaswi, M. (2023, February). A scalable network intrusion detection system using bi-lstm and cnn. In *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)* (pp. 1-6). IEEE.

[25] Kanumalli, S. S., Mantena, S. J., Kandula, S., Doppalapudi, K., & Atluri, T. (2022, May). Automated Irrigation Management System using IoT. In *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 476-482). IEEE.

[26] Kanumalli, S. S., Swathi, S., Sukanya, K., Yamini, V., & Nagalakshmi, N. (2022). Classification of dna sequence using machine learning. In *Soft Computing for Security Applications:*

[27] Prathipati, Silpa Chaitanya, and Susanta Kumar Satpathy. "A Multilevel De-Noising Approach for Precision Edge-Based Fragmentation in MRI Brain Tumor Segmentation." *Traitement du Signal* 40.4 (2023): 1715.

[28] Prathipati, Silpa Chaitanya, and Susanta Kumar Satpathy. "Transforming 3D Brain Tumour Image Segmentation: An Enhanced V-Net Approach for Precise Diagnosis and Treatment Planning." *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*. IEEE, 2024.

[29] Chaitanya, Kosaraju, et al. "Ads Click-Through Rate prediction using Attention based LSTM Mechanism." 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2024.

[30] Sujatha, V., Prasanthi, Y., Pravallika, C.H., ... Ayesha Banu, S.K., Sahithi, M.,K(23)

[31] " A Computer Vision Method for Detecting the Lanes and Finding the Direction of Traveling the Vehicle*Lecture Notes in Networks and Systems*", 2023, 612, pp. 373–382

[32] Sri, L. Akhila, K. Manvitha, G. Amulya, I. Sai Sanjuna, and V. Pavani. "FBI crime analysis and prediction using machine learning." *Journal of Engineering Sciences* 11, no. 4 (2020): 441-448.

[33] P. V, L. S. K, P. Vyshnavi A, M. Ch and S. B. G, "Students Community Portal using Machine Learning," *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 2023, pp. 1109-1113, doi: 10.1109/ICEARS56392.2023.10085516.

[34] Sirisha, Aswadati, et al. "Intrusion detection models using supervised and unsupervised algorithms-a comparative estimation." *International Journal of Safety and Security Engineering* 11.1 (2021): 51-58.

[35] Krishna, KVSS Rama, et al. "Vehicle Number Plate Detection using Deep Learning." *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)*. IEEE, 2024.

[36] Krishna, Komanduri Venkata Sesha Sai Rama, et al. "Classification of Glaucoma Optical Coherence Tomography (OCT) Images Based on Blood Vessel Identification Using CNN and Firefly Optimization." *Traitement du Signal* 38.1 (2021).

[37] Rayachoti, Eswaraiah, Sudhir Tirumalasetty, and Silpa Chaitanya Prathipati. "Watermarking system for telemedicine based on FABEMD." *Multimedia Tools and Applications* 81.30 (2022): 44383-44404.

[38] Chaitanya, P. Silpa, KV Narasimha Reddy, and G. Madhavi. "Effective Search of Color-Spatial Image Using Semantic Indexing." *International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol* 2 (2012): 9-19.

[39] Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Veeneetha, S. V., Srivalli, N., ... & Sahitya, D. (2022, November). Prediction of Flight-fare using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 134-138). IEEE.

[40] Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Bhargavi, P. J., Alekhya, A., ... & Nandini, K. (2022, November). Cardiovascular Disease Prediction using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 60-66). IEEE.

[41] Srikanth Kilaru " A Novel Approach to Human Iris Recognition And Verification Framework Using Machine Learning Algorithm" 2023 6th International Conference on Contemporary Computing and Informatics (IC3I),

[42] DOI: 10.1109/IC3I59117.2023.10397886, ISBN Information:Electronic ISBN:979-8-3503-0448-0

Print on Demand(PoD) ISBN:979-8-3503-0449-7

[43] Srikanth Kilaru "Analytical models for collaborative autonomous mobile robot solutions in fulfillmentcenters" in Applied Mathematical Modelling,Volume 91, March 2021, Pages 438-457,https://doi.org/10.1016/j.apm.2020.09.059

[44] Gopi, A. P., & Naik, K. J. (2022). An IoT model for fish breeding analysis with water quality data of pond using modified multilayer perceptron model. *2022 International Conference on Data Analytics for Business and Industry (ICDABI)*, 448-453. https://doi.org/10.1109/ICDABI56818.2022.10041617

[45] Arepalli, P. G., & Naik, K. J. (2024). A deep learning-enabled IoT framework for early hypoxia detection in aqua water using lightweight spatially shared attention-LSTM network. *Journal of Supercomputing*, *80*(2), 2718-2747. https://doi.org/10.1007/s11227-023-05580-x

[46] Arepalli, P. G., & Naik, K. J. (2023). An IoT-based water contamination analysis for aquaculture using lightweight multi-headed GRU model. *Environmental Monitoring and Assessment*, *195*(12), Article 1516. https://doi.org/10.1007/s10661-023-12126-4

[47] Gopi, A. P., Gowthami, M., Srujana, T., Gnana Padmini, S., & Durga Malleswari, M. (2023). Classification of denial-of-service attacks in IoT networks using AlexNet. In *Smart Innovation, Systems and Technologies* (Vol. 316, pp. 349-357). https://doi.org/10.1007/978-981-19-5403-0_30

[48] Bikku, T., Gopi, A. P., & Prasanna, R. L. (2019). Swarming the high-dimensional datasets using ensemble classification algorithm. In *Advances in Intelligent Systems and Computing* (Vol. 815, pp. 583-591). https://doi.org/10.1007/978-981-13-1580-0_56