Journal of Science, Computing and Engineering Research (JSCER)
Volume-6, Issue- 9, October 2023.
DOI: *https://doi.org/10.46379/jscer.2023.060903*

# Efficient Finger Print Forgery Detection in Personal Care System

**Anuar, Mohd Ariffin, Shamsuddin, Faizal**

Assistant Professor, Department of ECE, Faculty of Engineering, College of Putra Malaysia, Serdang.

**Article Information**

Received : 06 Sep 2023
Revised : 14 Sep 2023
Accepted : 10 Sep 2023
Published : 16 Oct 2023

*Corresponding Author:*
*Anuar*

**Abstract—**Various medical organizations maintain records of different patients which has more sensitive data which has to be secured from illegal access. Even the finger prints has been used as key there are malformed users who can try to intrude the system and steal information. So detection the forged finger prints becomes more essential. Number of approaches available for the detection of forged prints, they does not produce efficient results in forgery detection. Towards the problem of forgery detection, an efficient Region Based Minutiae Mass Measure (RMMM) approach is presented towards support the security of health care systems. The user has been validated with general information and the finger print has been captured through the capturing device. The method first enhances the input finger print image by applying gabor filter to remove the noise. The same has been performed in the input test image and based on the minutiae mass value, the forged print has been detected. The method has produced efficient results on forged finger print detection and improves the classification accuracy.

**Keywords:** ***Finger Print, Authentication Systems, Minutiae, MMM, Forgery Detection, Health Care Systems***



**Citation: Anuar, Mohd Ariffin, Shamsuddin, Faizal** "Efficient Finger Print Forgery Detection in Health Care System, 6(9), 1-17, October 2023.

## I. INTRODUCTION

The organizations maintain various resources in their resource pool and would contain various information related to their customers and employees. Such data has to be restricted and safeguard from illegal access. To perform the restriction, there are number of protocols has been used earlier. The password based approach has been used in earlier days. Such methods are very poor in restriction because the leakage of password would allow the illegal access. To improve the performance there are many Manuscript published on 30 December 2019. *Correspondence Author(s) A. Vinoth, Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore (Tamilnadu), India. Dr.S. Saravanakumar, Associate Professor, Department of Computer Science Engineering, Shanmuganathan Engineering College, Arasampatti (Tamilnadu), India. © The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/ approaches being discussed in the last decade. The modern security systems have used various biometric features in restricting the users from illegal access. The biometric features being used are, eyes, lips, nose, face, finger prints, palm print and so on. The most health care organizations maintain their patient information in a centralized or a distributed data base. Such data can be accessed by their own employees and users. However, there are number of information of patients which has to be restricted from different users and the organization is more responsible for the leakage of user personal information. So restricting the malformed access is becomes more important and the system has to enforce higher access restrictions. In this case the biometric features can be used. However, there are number of biometric features used for the access restriction and to verify the identity of the users, the finger print has some special features. The features of the finger print will not be correlate or match with the others and it is identical even between twins. Such finger print has been used in the recent days for the identity management and access restriction. In general, the finger prints are not change according to age and will be retain in the same condition till death. The structure of the finger print would change due to cuts and scars on the finger. Using all these features the process of finger print matching can be performed. In general the matching of finger print has been performed according to the features of finger print. The matching process would consider either one or two features. But it is necessary to consider all the features in the matching process. This paper introduces an efficient approach towards the classification of finger print and to identify the forgery one. Before moving to the technical aspects, it is necessary to mind few facts. In any print image, the number of edges, ends, bifurcation, island and dots are appearing in a limit. When a malicious user generates a fake one, it will not appear similarly. From the fake finger print, you can identify the characteristics or features and based on their appearance, its trustworthy can be measured. The Minutiae mass measure (MMM) is estimated based on their count and their

gray mass value. The detailed approach is discussed in the next section. The RMMM measure represent the minutiae mass measure estimated on each region of the image.

## II. RELATED WORK

There are number of methods have been discussed for the detection of forged finger prints. This section discuss about few of them. A support vector machine with kernel has been used for the classification of finger prints in [1]. The method uses finger print data set and has been presented towards the usage in access restriction, user verification in ATM and criminal identification process. The method has produced efficient results in altered finger print identification. In [2], the author performs an analysis on fake finger prints and conclude that the image quality software is not suitable in detecting the altered prints in efficient manner. It has been identified that the image quality does not change because of alteration in the finger prints. Toward the detection of altered finger print an efficient approach is presented. The method uses the distribution of minutiae and detect the finger prints based on the orientation fields of the image. Based on the distribution value the fake prints are identified. A novel approach to fingerprint identification using method of sectorization [3], introduce a complete (fullyimplemented) algorithm for fingerprint recognition. The work describes image preprocessing based on our previous works and feature vector creation that bases on sectoralization. The image preprocessing includes filtering, skeletonisation, minutiae extraction by CN (Crossing Number) algorithm and spurious minutiae removal. The feature vector creation is based on dividing the fingerprint into sectors. The division is done on the basis of image height. Altered fingerprint detection – algorithm performance evaluation [4], present a comparative study on the performance of altered fingerprint detection algorithms. Different algorithms from different institutions have been evaluated on two different datasets. Both datasets feature real alterations on fingers and the ground truth regarding the alteration is known a priori, as, in some cases, corresponding pre-altered fingerprints were also available. In [5], an synthetic alteration on the finger prints has been generated artificially and the generated finger prints are used to evaluate the performance of various finger print analysis approaches. This supports the research of finger print alteration detection by providing dataset to the researchers. Similarly in[6], an efficient approach has been proposed and has been validated with the dataset generated. In [7], an orientation based altered finger print identification and detection has been presented. In [8], the author performs a survey on attack detection methods which detects altered finger prints. As the biometrics are mostly used in overall systems for the restriction and authentication of different users, the malicious users tries to access the system by generating fake finger prints. There are number of approaches available to perform altered finger print detection and the author performs a detailed survey on the methods. In Critical Analysis and Detection of Altered Fingerprints [9], the author performs optimization of image quality based algorithm in altered finger print. The method uses neuro fuzzy in the detection of altered finger print and the fuzzy rule has been generated using image database. An investigation of fake fingerprint detection approaches [10], the author perform a detailed review on various methods of fake finger print detection. Number of research articles has been considered and based on that various taxonomy of fake prints has been generated. In [11], a gradient texture based altered finger print detection algorithm is presented. The method extracts the co-occurrence matrix and gradient features from the image. Based on the features extracted, the multi order gradient features are generated to identify the altered finger print detection. Towards the detection of spoofing attack by altered finger print, an efficient approach is presented based on counter measures in [12]. In [13], CNN feature based finger print liveliness detection is presented. The method initially segments the input image and using the segmented image, the distribution of various features has been identified. The distribution measures have been used to perform altered finger print detection. In [14], the quality features has been used to perform spoofed or altered finger print detection. The method considered the Gabor feature, frequency of ridges, direction map and frequency filed. Based on the above mentioned features, the method performs altered finger print detection. Similarly in [15], the same set of features has been considered and evaluated using large data set. In [16], a minutiae match algorithm using divide and conquer approach is presented to identify the altered finger print. The method divides the image into different sections and for each section the method matches the minutiae with the template available. Based on that the altered finger print has been detected and produces efficient results. In [17] a security protocol for the securing of health care record using biometric is presented. The method considers the advantages, disadvantages, and ethical consequences of utilizing biometric technology to secure the electronic health record in regards to cost, usability, accessibility, and accuracy. In addition to evaluating the primary application, the essay acknowledges the potential use of biometric technology to identify patients by vasculature scanning in the future.

## III. FINGER PRINT DETECTION

The proposed minutiae mass measure based approach performs noise removal and then enhances the input finger print image. Second, the image has been split into number of regions and for each region, the method extracts various ridge features. Based on extracted features the MMM value has been measured to perform classification. The detailed approach is presented in this paper.

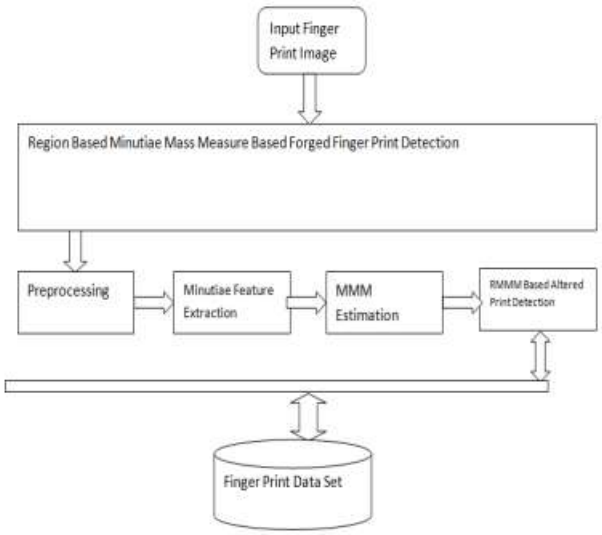


**Figure 2: Architecture of Proposed RMMM Based Forged Finger Print Detection System**

. The Figure 1, shows the architecture of proposed region based forged finger print detection algorithm which uses MMM measure. Preprocessing At this stage, the input image has been read and gabor filter has been applied to remove the noise introduced by the capturing device. The noise removed image has been applied with the sharpening techniques to improve the quality of image. The quality improved image has been used to extract the features from the image. Algorithm Input: Image Img Output: Preprocessed Image Pimg Start Read input finger print image Img Initialize Gabor Filter GF. For each level of Gf Pimg = Apply GF(l, Img) End Stop The above discussed algorithm removes the noise from the image by applying multi level Gabor filter. The noise removed image has been used to perform minutiae feature extraction in the next stage. Minutiae Feature Extraction In this stage, the quality improved image has been read and has been split into number of sectional images. From each sectional image, the method extracts the features of ridge like minutiae island, minutiae dots, ends, enclosures, and bifurcation. Extracted features are converted into feature vector which will be used to estimate the MMM measure in the next stage. Algorithm Input: Enhanced Image EI Output: Feature Vector Fv. Start Read enhanced image EI. Split image into sectional image. SI = ∫ split(EI, < $Sa$, $Ea$ > Nos i=1 Nos – no of sections or regions Sa – Starting angle Ea- Ending angle. For each sectional image Si Extract Minutiae island Mi = ∑ Islands ∈ Si Extract Minutiae dots Md = ∑ Dots ∈ Si Extract Minutiae End Me = ∑ End ∈ Si Extract Minutiae enclosures Men = ∑ Enclosures ∈ Si Extract Minutiae Bifurcation Mb = ∑ Bifurcation ∈ Si Construct feature vector Fvi = {Mi, Md,Me, Men, Mb} Add to feature vector Fv = ∑(Fvk ∈ Fv) ∪ Fvi End Stop The feature extraction algorithm extracts various features from each sectional image and add to the feature vector.

## IV. RESULT AND DISCUSSION

The proposed algorithm has been implemented using Matlab and has been evaluated for its efficiency in the classification. The proposed algorithm has produced efficient results on the forged finger print detection and improves the performance of classification. The efficiency of the method has been evaluated and compared with other methods. The proposed method has produced the following results.

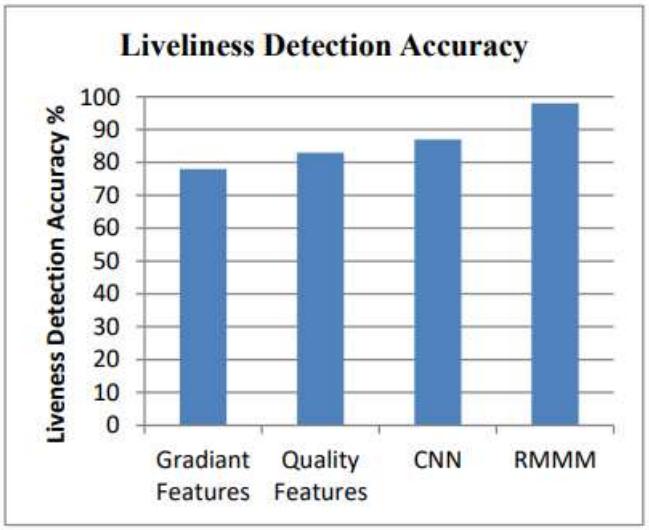


**Figure 4: Comparison on Liveliness Detection Accuracy**

## V. CONCLUSION

detection with minutiae mass measure is presented. The method reads the input image and removes the noise from the image. Then the method improves the image quality by sharpening the image. Third, the image has been split into number of sectional images and from each image the method extracts various features of minutiae. Using the features extracted the method estimates the MMM value with each subsequent region feature of the feature set available in the data set. If the similarity between any of the region according to the similarity false below the threshold then it has been considered as the region has been altered and the image has been considered as forgery print image. The proposed algorithm has improved the performance of forgery detection and reduces the false ratio and time complexity as well

## REFERENCES

[1]. P. Nirmala, T. Manimegalai, J. R. Arunkumar, S. Vimala, G. Vinoth Rajkumar, Raja Raju, "A Mechanism for Detecting the Intruder in the Network through a Stacking Dilated CNN Model", Wireless Communications and Mobile Computing, vol. 2022, Article ID 1955009, 13 pages, 2022. https://doi.org/10.1155/2022/1955009.

[2]. J.R.Arunkumar, Dr.E.Muthukumar,"A Novel Method to Improve AODV Protocol for WSN" Journal of Engineering Sciences" Volume 3, Issue 1, Jul 2012. ISSN NO: 0377-9254

[3]. J. R. Arunkumar, S. Velmurugan, B. Chinnaiah, G. Charulatha, M. Ramkumar Prabhu et al., "Logistic regression with elliptical curve cryptography to establish secure iot," Computer Systems Science and Engineering, vol. 45, no.3, pp. 2635–2645, 2023.

[4]. P. K. Devi, D. Arulanantham, C. Kalaivanan, N. Gomathi, J. R. Arunkumar and G. Ramkumar, "An Secure and Low Energy Consumption based Intelligent Street Light Managing System using LoRa Network," 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, 2022, pp. 638-645, doi: 10.1109/ICECA55336.2022.10009408.

[5]. Prathima Chilukuri , J.R. Arun Kumar , R. Anusuya , M. Ramkumar Prabhu. "Auto Encoders and Decoders Techniques of Convolutional Neural Network Approach for Image Denoising In Deep Learning" Journal of Pharmaceutical Negative Results, 13(4), 1036–1040. https://doi.org/10.47750/pnr.2022.13.04.142 ,November 4, 2022.

[6]. R. Yugha, V. Vinodhini, J. R. Arunkumar, K. Varalakshmi, G. Karthikeyan and G. Ramkumar, "An Automated Glaucoma Detection from Fundus Images based on Deep Learning Network," 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dharan, Nepal, 2022, pp. 757-763, doi: 10.1109/I-SMAC55078.2022.9987254.

[7]. E. Thenmozhi, A. Karunakaran, J. R. Arunkumar, V. Chinnammal, C. Kalaivanan and G. Anitha, "An Efficient Object Detection and Classification from Restored Thermal Images based on Mask RCNN," 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dharan, Nepal, 2022, pp. 639-645, doi: 10.1109/I-SMAC55078.2022.9987422.

[8]. L. Saravanan, W. Nancy, K. P. Chandran, D. Vijayanandh, J. R. Arunkumar and R. T. Prabhu, "A Novel Approach for a Smart Early Flood Detection and Awareness System using IoT," 2022 8th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2022, pp. 1-4, doi: 10.1109/ICSSS54381.2022.9782286.

[9]. S. Bharathi, A. Balaji, D. Irene. J, C. Kalaivanan and R. Anusuya, "An Efficient Liver Disease Prediction based on Deep Convolutional Neural Network using Biopsy Images," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 1141-1147, doi: 10.1109/ICOSEC54921.2022.9951870.

[10]. Prathima, C. H., Anusuya, R., & Prabhu, M. R. K. (2022). Comprehensive Design Analysis of Digital Marketing in Agriculture Sector. International Journal of Early Childhood Special Education, 14(5), 2022.

[11]. Atul Kumar Dwivedi, Deepali Virmani, Anusuya Ramasamy,Purnendu Bikash Acharjee, Mohit Tiwari" Modelling And Analysis Of Artificial Intelligence Approaches In Enhancing The Speech Recognition For Effective Multi-Functional Machine Learning Platform – A Multi Regression Modelling Approach " Journal of Engineering Research - ICMET Special Issue, 2022-04-06.

[12]. M.Ramkumar Prabhu, A.Rajalingam, J.R.Arunkumar, Dr.R.Anusuya" Microstrip Patch Antenna Using Combined Slots for Bandwidth Enhancement and Size", Journal of Engineering Sciences, Vol 11, Issue 1, Jan, 2020, ISSN NO: 0377-9254.

[13]. Anusuya Ramasamy, Abel Adane Changare" Hybrid Fuzzy Knowledge Based Prediction Model for the Software Development and Maintenance Quality in Software Engineering Approach" International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-9 Issue-10, August 2020.

[14]. J.R.Arunkumar," Chaotic African Buffalo Optimization Based Efficient Key Mechanism in Categorized Sensor Networks:, International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-9 Issue-3, February, 2020.

[15]. R. Anusuya, M. Ramkumar Prabhu, Ch. Prathima, J. R. Arun Kumar" Detection of TCP, UDP and ICMP DDOS attacks in SDN Using Machine Learning approach" Journal of Survey in Fisheries Sciences, Vol. 10 No. 4S (2023): Special Issue 4.

[16]. M.Ramkumar Prabhu, A.Rajalingam, J.R.Arunkumar, R.Anusuya, "Microstrip Patch Antenna Using Combined Slots For Bandwidth Enhancement And Size" Journal of Engineering Sciences (JES),Vol 11, Issue 1, Jan / 2020, ISSN NO: 0377-9254.

[17]. M.Ramkumar Prabhu, J.R.Arunkumar, A.Rajalingam, R.Anusuya "A Modified Square Patch Antenna with Rhombus slot for High bandwidth" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-9, July 2019.

[18]. Revanesh, M., Gundal, S.S., Arunkumar, J.R.Arunkumar et al. Artificial neural networks-based improved Levenberg–Marquardt neural network for energy efficiency and anomaly detection in WSN. Wireless Netw (2023). https://doi.org/10.1007/s11276-023-03297-6.

[19]. I. Chandra, K. V. Karthikeyan, R. V, S. K, M. Tamilselvi and J. R. Arunkumar, "A Robust and Efficient Computational Offloading and Task Scheduling Model in Mobile Cloud Computing," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ICECONF57129.2023.10084293.

[20]. Jangam Raghunath, S Kiran, G Siva Nageswara Rao, JR Arun Kumar, R Anasuya, C Siva Kumar," A MACHINE LEARNING TECHNIQUE TO DETECT BEHAVIOR BASED MALWARE", Semiconductor Optoelectronics, Vol. 42 No. 1 (2023), 1268-1278

[21]. Dr.J.R.Arunkumar. "Enhanced Dynamic Authorized Secured Protocol for Wireless Sensor Networks, "Journal of Science, Computing and Engineering Research, 1(1), 07-11, Mar-Apr 2020.

[22]. Anitha Gopalan,O. Vignesh,R. Anusuya,K. P. Senthilkumar,V. S. Nishok,T. Helan Vidhya, Florin Wilfred," Reconstructing the Photoacoustic Image with High Quality using the Deep Neural Network Model", Contrast Media & Molecular Imaging, Volume 2023 | Article ID 1172473 | https://doi.org/10.1155/2023/1172473.

[23]. R. Anusuya, N. Anusha, V. Sujatha, R. Radhika and S. Iniyan, "Machine Learning based Landslide Detection System," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 319-323, doi: 10.1109/ICCMC56507.2023.10084226.

[24]. S. Sivakumar, R. Anusuya, V. Nagaraju, L. P. Narendruni and R. Thamizhamuthu, "QoS Based Efficient Link and Consistent Routing in Wireless Sensor Network," 2023 International Conference on Intelligent and Innovative

Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 1241-1246, doi: 10.1109/IITCEE57236.2023.10091080.

[25]. I. Chandra, G. Sowmiya, G. Charulatha, S. D, S. Gomathi and R. Anusuya, "An efficient Intelligent Systems for Low-Power Consumption Zigbee-Based Wearable Device for Voice Data Transmission," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10083856.

[26]. R. Meena, T. Kavitha, A. K. S, D. M. Mathew, R. Anusuya and G. Karthik, "Extracting Behavioral Characteristics of College Students Using Data Mining on Big Data," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10084276.

[27]. G. Karthikeyan, D. T. G, R. Anusuya, K. K. G, J. T and R. T. Prabu, "Real-Time Sidewalk Crack Identification and Classification based on Convolutional Neural Network using Thermal Images," 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2022, pp. 1266-1274, doi: 10.1109/ICACRS55517.2022.10029202.

[28]. S. Bharathi, A. Balaji, D. Irene. J, C. Kalaivanan and R. Anusuya, "An Efficient Liver Disease Prediction based on Deep Convolutional Neural Network using Biopsy Images," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 1141-1147, doi: 10.1109/ICOSEC54921.2022.9951870.

[29]. Dr. R.Anusuya. ―Stacking Dilated CNN Authorized Secured Protocol for IoT Security, ―Journal of Science, Computing and Engineering Research, 1(1), 01-07, May- June 2022.