

RESEARCH ARTICLE

Multi-region minutiae depth value-based efficient forged finger print analysis

M. Baskar¹, Renuka Devi Rajagopal², PRASAD B. V. V. S.³, J. Chinna Babu^{4*}, Gabriela Pajtinková Bartáková⁵, T. S. Arulananth⁶

1 Department of Computing Technologies, School of Computing, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamilnadu, India, **2** School of Computer Science and Engineering, VIT University, Chennai, Tamilnadu, India, **3** School of Engineering (CSE), Anurag University, Hyderabad, India, **4** Department of Electronics and Communication Engineering, Annamacharya Institute of Technology and Sciences, Rajampet, AP, India, **5** Faculty of Management, Comenius University in Bratislava, Bratislava, Slovakia, **6** Department of Electronics and Communication Engineering, MLR Institute of Technology, Hyderabad, India

* jchinnababu@gmail.com

OPEN ACCESS

Citation: Baskar M, Rajagopal RD, B. V. V. S. P, Babu JC, Bartáková GP, Arulananth TS (2023) Multi-region minutiae depth value-based efficient forged finger print analysis. PLoS ONE 18(11): e0293249. <https://doi.org/10.1371/journal.pone.0293249>

Editor: Bhisham Sharma, Chitkara University, INDIA

Received: August 19, 2023

Accepted: October 9, 2023

Published: November 16, 2023

Copyright: © 2023 Baskar et al. This is an open access article distributed under the terms of the [Creative Commons Attribution License](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Data Availability Statement: All relevant data are within the paper and [Supporting Information](#).

Funding: The authors extend their appreciation to Gabriela Pajtinková Bartáková, Faculty of Management, Comenius University in Bratislava, Odbojárov 10, 82005 Bratislava 25, Slovakia for providing the funding for this Manuscript.

Competing interests: The authors have declared that no competing interests exist.

Abstract

The application of biometrics has expanded the wings to many domains of application. However, various biometric features are being used in different security systems; the fingerprints have their own merits as it is more distinct. A different algorithm has been discussed earlier to improve the security and analysis of fingerprints to find forged ones, but it has a deficiency in expected performance. A multi-region minutiae depth value (MRMDV) based finger analysis algorithm has been presented to solve this issue. The image that is considered as input has been converted into noisy free with the help of median and Gabor filters. Further, the quality of the image is improved by sharpening the image. Second, the preprocessed image has been divided into many tiny images representing various regions. From the regional images, the features of ridge ends, ridge bifurcation, ridge enclosure, ridge dot, and ridge island. The multi-region minutiae depth value (MRMDV) has been computed based on the features which are extracted. The test image which has a similarity to the test image is estimated around MRMDV value towards forgery detection. The MRMDV approach produced noticeable results on forged fingerprint detection accuracy up to 98% with the least time complexity of 12 seconds.

1. Introduction

Various organizations have used the development of information technology to meet their goals. As the organizations have a variety of information on their system, which belongs to different users and business partners, they are responsible for securing the data most effectively. Any organization faces various challenges against the data maintained through threats. The security measures which can be different are enforced to secure the data and handle the problem of illegal access. Access restriction is the most dominant one, which restricts the illegal user from accessing the available data. In this way, different approaches are used, like profile-

based access and key-based access restriction methods. However, the performance of such methods is not efficient in meeting the system's security requirements as they can be tampered with easily by various adversaries. Using biological features is more effective in enforcing such security systems. The facial features and thumb features are more challenging for the adversary that can support such security systems. Fingerprints and palm prints can be used towards the problem effectively.

Human fingerprint has great independence among other features of biometrics. It has unique characteristics which vary between any number of users. It has components of Minutiae ending, bifurcation, islands, dots, and so on. These components can be common in all human fingerprints but vary in numbers and sizes. The components and their numbers can be obtained by processing the fingerprint image. These numbers will not correlate with any other numbers. So, by adopting such finger analysis in security systems, the performance of authentication and illegal access restriction can be enforced most strictly.

The picture of the sample fingerprint is presented in Fig 1, which has both original and altered fingerprints. The adversary or malformed user would try to breach the security walls by producing an altered print to the system. However the system should be capable of differentiating the original and altered one. So, the security system should consider various features from the ridge like dots, islands, ends, enclosure, and bifurcation. By considering such features in the authentication and verification process, the problem of forgery detection can be handled effectively.

Adapting finger print analysis to organizational security is a highly required process. Because finger print is the most unique feature for any human, and by including such feature for security reasons improves the security of any organization. However, there are adversaries who would produce forged finger print for the system and the system should be more rigid in detecting such forged finger prints. If the system is highly efficient in detecting forged finger prints then the security performance of the system will be highly efficient. This would be used in many security applications from banks to the defense sector.

This score presents an efficient Multi Region Minute Depth Value-Based Efficient Forged Finger Print Analysis model in this article. The model considers the depth of each feature in different regions to perform the verification process. The model estimates the Minutiae Depth Value (MDV) according to the number of features present and their instances with the mass value. By computing such MDV values for various regions, the method computes MRMDV values to classify the fingerprint. The multi-region minutiae depth value (MRMDV) has been computed based on the features which are extracted.

Unlike other methods, the proposed MRMDV based scheme consider various features like ridge ends, ridge bifurcation, ridge enclosure, ridge dot, and ridge island being extracted from various regions of the image. By extracting features from various region and concerning various regional features, the localization of the features are obtained accurately and supports the performance development in forgery detection.

1.1 Highlights and problem statement

- Organizational security has been approached by using finger print analysis.
- Forged finger print detection plays vital role in authenticating the persons in the organization.
- The existing methods consider a minimum set of features in detecting forgery in finger print, which in turn produces a higher false ratio.



Fig 1. Sample altered fingerprints.

<https://doi.org/10.1371/journal.pone.0293249.g001>

- The previous methods do not concern the entire features of finger print towards forgery detection.
- The forgery detection is approached with the multi-region minutiae depth value (MRMDV) based approach.
- The method considers regional features of finger print images and supports the achievement of higher accuracy in forgery detection.

The article has been organized to present the introduction, problem statement, highlights and motivation in section 1. Section 2 details the objective of the paper and Section 3 presents the detailed literature survey of the problem and Section 4 presents the contribution of the paper. Section 5, details the complete working model of the proposed system. Section 6 presents the experimental results obtained from the proposed method and presents the comparative study. Section 7, presents the conclusion of the proposed work.

2. Objectives

The problem of forgery detection in the fingerprints is analyzed and studied well. The presence of forgery has been identified according to the minutiae features. Any minutiae contain many edges, junctions, bifurcation, and so on. Different methods are available in the literature that consider just the ridge end, edge, dot, enclosures, and bifurcations. But there is no such method that considers the maximum possible features in measuring the similarity towards classification. On the other side, the classification approaches consider the entire print and measure the similarity among the features. But the noise generated by the capturing device or any scare generated on the finger of any person would generate missing features. This introduces higher false classification and affects the performance of classification. This encourages the author to design an efficient approach towards forged fingerprint detection.

3. Related work

This section details various methods of fingerprint analysis for forged print detection.

In [1], a fingerprint classification approach is discussed with the use of SVM. The method has been designed to enforce access restriction and verification in crime departments. The method has improved the verification performance.

In [2], a fake fingerprint detection approach is presented, which uses minutiae feature distribution to detect the fake prints according to the orientation features. Similarly, in [3], the author introduced an efficient altered print detection that uses a crossing number minute extraction algorithm. The method splits the images into sectors to extract the features in measuring the similarity between them.

In [4], the analysis of the performance evaluation of various altered fingerprint detection schemes is discussed to present the comparative study. The performance of different fingerprint analysis approaches is evaluated by generating fingerprints artificially to support various research sectors [5]. Such generated data set has been validated by different approaches in [6]. Similarly, an orientation-based approach is presented in [7] towards the problem.

In [8], they analyze how the biometric features obtained from fingerprints are used in access restriction in different control systems. Also, the author presents a comparative study on various fake print detections. In [9], a neuro-fuzzy-orient approach is presented [9], which generates a number of fuzzy rules from the image data set to support classification.

In [10], the author presents a detailed analysis of various fingerprint analysis schemes and fake print detection schemes. Also, a taxonomy of approaches is generated. Similarly, a texture-based approach to fake print detection is presented in [11], which generates a co-occurrence matrix based on the gradient features toward classification.

In [12], a counter-measure-based spoofing attack detection scheme with an altered fingerprint is discussed. Similarly, a CNN model is presented in [13] for the detection of the liveness of fingerprints. The method extracts the feature distribution by segmenting the image and estimates distribution measures to perform detection. The presence of a spoofed attack is handled with the quality features in [14], which consider the Gabor feature, ridge frequency, and so on. Such features are used in the classification. The features discussed above have been used to evaluate different data sets in [15].

A divide and conquer-based minutiae matching is sketched in [16] to detect fake fingerprints. The method generates sub-samples and matches them with the minutiae using the template matching algorithms.

In [17], the author presented a recognition system that acquires the fingerprint and preprocesses the image by binarization. The feature from the binarized image is extracted using a minutiae extractor to collect the ridge edge and bifurcation. According to the features extracted, feature matching and recognition are performed. The verification is performed by measuring the distance among the minutiae.

In [18], a detailed skeleton of CNN-based deep learning framework for crime scene detection is presented, which uses the data sets that contain several photographs that are incomplete, and the method extracts the minutiae and classifies them according to the CNN available. In [19], a fake print analysis approach is presented, which analyzes different images obtained from different sensors. The images from optical and thermal sensors are obtained, and by using the Min-max approach, the normalization is performed. From the normalized images, the method extracts GLCM (Gray Level Co-Occurrence Matrix) image features and is classified with KNN and SVM.

In [20], the author designed an efficient technique to detect forged fingerprint images. The recognition is performed with the Boltzmann machine. The problem of fake fingerprint detection is approached with a Fuzzy Inference System (FIS) with ANN [21] to improve the classification performance. In the Research [21] the authors established a region centric based RCMPM finger print recognition approach. Similarly, a touch-based biometric authentication

system is presented for forgery attacks [22]. The method performs authentication by using a behavior-based approach to find the secret values. A rapid forgery detection scheme is presented in [23], which identifies the dissimilar blocks between the forged one and the normal one. The method computes the dissimilarity between the prints by searching the blocks in forged ones. Euclidean measures are computed towards classification, where the images are applied with morphological operation and binarization.

This paper [24] presents a methodology for quantifying heart rate using a fingertip and Arduino microcontroller. The technique is founded upon the principle of Photo Plethysmography (PPG), a non-invasive approach for quantifying changes in tissue blood volume employing a light source and detector. During cardiac activity, the heart facilitates blood circulation throughout the entire body, resulting in fluctuations in blood volume within the finger artery. The detection of blood fluctuation can be achieved by employing an optical detecting mechanism near the fingertip. The signal is capable of being amplified and afterward transmitted to an Arduino microcontroller through the utilization of serial port connectivity. Heart rate monitoring and counting are conducted using data processing technology.

This study [25] introduces a novel approach for detecting and eliminating shadows, explicitly addressing the issue of counterfeit shades. The proposed method leverages the HOG (Histogram-of-Oriented Gradients) characteristics to achieve effective results. During the initial phase of moving object identification, the Gaussian Mixture Model (GMM) is employed to segregate the foreground regions accurately. Using the HSV color space enhances the differentiation between chromaticity and intensity, hence facilitating the identification of shadows within the fragmented context. However, it is essential to note that this approach may inadvertently misclassify certain portions of objects as shadow regions. The utilization of the observed phenomenon that object regions, specifically incorrectly categorized places and fake shadows, significantly alter the background data. This contrasts casting shadows, which primarily induce intensity variations across the background. They employ a local feature-matching technique to distinguish between genuine and counterfeit shadow regions accurately. Once the areas have been determined, it becomes feasible to eliminate the shadows present in the object regions without compromising any information. The experimental findings demonstrate that the suggested approach yields favorable outcomes in outdoor environments.

The SVM based approach [1], considers only the limited features in the classification of finger print. The crossing minutiae extraction algorithm used in [3], generates sectional features in the detection of fake finger print, however considering only the minutiae features only. This introduces poor accuracy in the classification. The neuro-fuzzy approach [9], generates fuzzy rules from limited features which restrict the accuracy of fake print detection. The texture-based scheme [9], generates co-occurrence matrix from gradient features alone which leads to poor accuracy in fake print detection. The CNN model presented in [13], uses distributional measures in fake finger print detection, but suffers from poor accuracy as the feature distribution will vary on age. The FIS-ANN model [21], perform forgery detection according to region features but lacks to consider entire features [26–29]. All the above-discussed methods are not efficient in detecting fake fingerprints, which raises the requirement for efficient techniques to be modeled [30–32].

4. Contributions

- Towards maximizing the performance of forged fingerprint detection, a novel scheme is designed and discussed in this section.

- Unlike other methods, the proposed MRMDV model considers all possible features of the finger print.
- The method considers the features in various regions towards finger print analysis.
- Based on the features collected, the method computes MRMDV value against various features to support localization and classification.
- The method introduces higher accuracy in classification with less false ratio.

5. Methodology

The multi-region minutiae depth value-orient scheme applies a multi-level Gabor filter used to remove the noise from the given input image and thereby increase in the image quality. Further, the image has been cropped into tiny regions as per the size of the window that is considered for the evaluation. The features from each tiny regional image are extracted according to the features considered. By using the features that are extracted, this method can be used to estimate the MDV value to compute the MRMDV value to support the classification process.

Fig 2 shows the functional diagram of the MRMDV approach, and each component is discussed in this section.

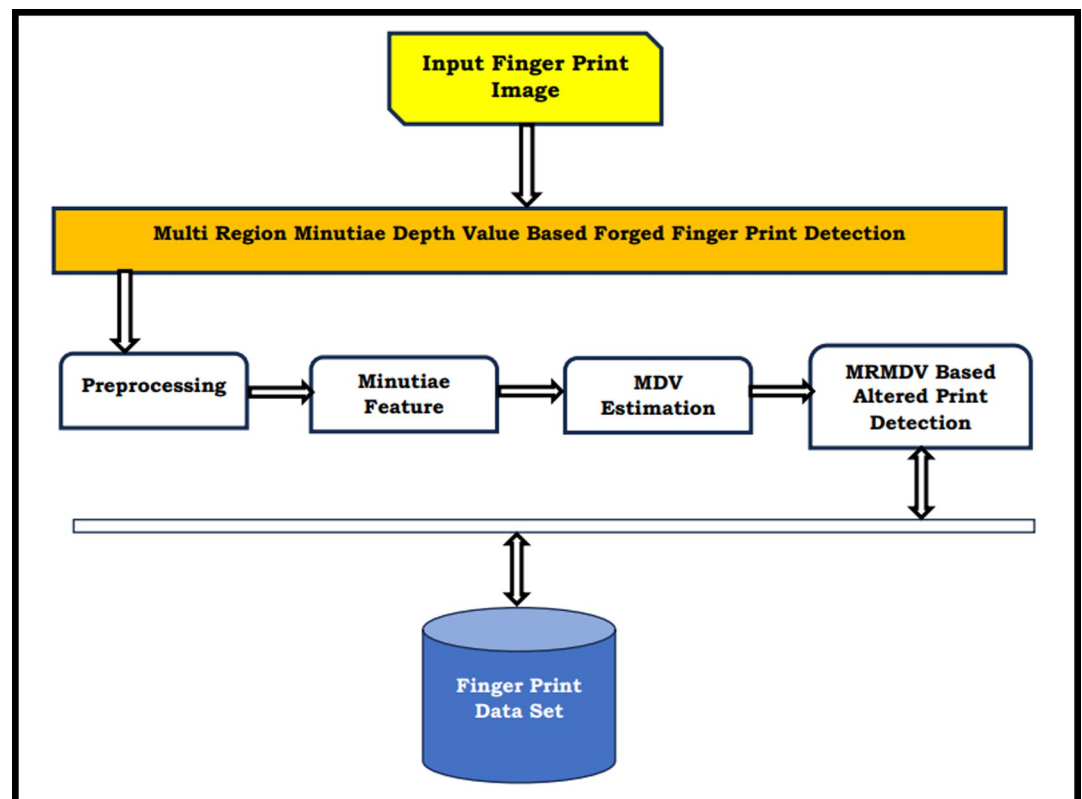


Fig 2. Structure of MRMDV-based forged finger print detection.

<https://doi.org/10.1371/journal.pone.0293249.g002>

5.1 Preprocessing

The image given has been applied with median and Gabor filters to remove the noise particles generated at capturing. The image, which is eliminated from the noise, is improved for its sharpness to enhance the image quality. The image with good quality is used in extracting the features of the image to support fake fingerprint detection.

Algorithm:

Given: Finger Print FP_Img

Obtain: Quality Improved image Qimg

Begin

Fetch Fpimg

NL

Gabor Filter GF = *Initialize* (GF, Coefficients).

$i = 1$

At all levels l

$Qimg = GF(I, FPIimg)$

At_End

Stop

The preprocessing approach applies the Gabor filter to eliminate the noisy parts and improve the image quality.

5.2 Minutiae feature extraction

The features of minutiae from the fingerprint image are extracted here. To perform this, the image is divided into a number of tiny images. By considering specific window size, the method crops the image into a number of regions. From the region images generated, the method extracts the concerned features. At each tiny part, the features of bifurcation, minutiae dots, Minutiae Island, ends, and enclosures are extracted. Obtained features are framed to form a feature vector to be utilized to compute MDV value.

Algorithm:

Given: Quality Improved Image Qimg

Obtain Feature Vector Set Fvs.

Begin

Fetch Quality Improved Image Qimg

Split image into regional image.

$$RI = \int_{i=1}^{Nos} \text{split}(EI, < Sa, Ea >$$

Nos--no of sections or regions

Sa--Starting angle

Ea- Ending angle.

From all regional images, Ri

$$\text{Obtain Minutiae Island Miland} = \sum_{i=1}^{Size(Ri)} [Islands \exists Ri]$$

$$\text{Obtain dots dot} = \sum_{i=1}^{Size(Ri)} [Dots \exists Ri]$$

$$\text{Obtain Ends Ed} = \sum_{i=1}^{Size(Ri)} [Ends \exists Ri]$$

$$\text{Obtain Enclosures Ens} = \sum_{i=1}^{Size(Ri)} [Enclosures \exists Ri]$$

$$\text{Obtain Bifurcation Bfn} = \sum_{i=1}^{Size(Ri)} [Bifurcation \exists Ri]$$

Generate feature vector Fv = { Miland, dot, Ed, Ens, Bfn }

$$Fvs = \sum (Fv \in Fvs) \cup Fv$$

Stop

The features of the finger image are extracted according to the minutiae in terms of bifurcation, enclosure, dot, island, and ends. The features obtained are converted to feature vectors in estimating MDV values.

5.3 MDV estimation

The Minutiae depth value (MDV) of any fingerprint shows the containment of mass ridge features. The value of MDV has been measured according to the frequency of dots, edges, bifurcation, ends, and enclosures. To measure the MDV value, the method counts the occurrence of all the features and estimates the frequency of each feature to compute the value of MDV. With the MDV value measured, the method performs the detection of altered print.

Algorithm:

Given: Feature Vector Fv

Obtain: MDV

Begin

Fetch Fv.

$$\text{Count Occurrence of dots } dc = \int_{i=1}^{\text{size}(Fv)} \text{Count}(Fv(i) \text{ type } == \text{dot})$$

$$\text{Count occurrence of Edge } Ec = \int_{i=1}^{\text{size}(Fv)} \text{Count}(Fv(i) \text{ type } == \text{edge})$$

$$\text{Count Occurrence of ends } Enc = \int_{i=1}^{\text{size}(Fv)} \text{Count}(Fv(i) \text{ type } == \text{End})$$

$$\text{Count Occurrence of enclosure } Encc = \int_{i=1}^{\text{size}(Fv)} \text{Count}(Fv(i) \text{ type } == \text{Enclosure})$$

$$\text{Count Occurrence of bifurcation } Bc = \int_{i=1}^{\text{size}(Fv)} \text{Count}(Fv(i) \text{ type } == \text{bifurcation})$$

$$\text{Measure Minute Depth } Md = \frac{Encc}{size(SI)} \times \frac{dc}{encc} \times \frac{ec}{bc}$$

$$\text{Measure Minute Depth Value MDV} = \frac{\sum MD}{size(Fv)}$$

Stop

The MDV estimation function measures the minutiae depth value according to the occurrence and frequency of all the features considered. The MDV value represents the similarity of the features on specific region of the image. This will be measured for all the regions of the image according to the region image generated and used to measure the final MRMDV value to support the classification.

5.4 MRMDV based altered finger print detection

The multi-region approach to fake fingerprint detection is conducted by measuring minutiae depth value for various regions of the print given. To handle this, first preprocessing is performed, which eliminates the noise and improves the quality of the image. Second, regional images are generated, and concern features are obtained. Third, from each regional feature obtained, the value of MDV is measured. Using the MDV value of all the regions, the value of MRMDV is measured to classify the fingerprint given.

Algorithm:

Given: Fingerprint image Fpi, Data set Ds.

Obtain: Boolean

Begin

 Read Input image Fpi

 Read data set Ds.

 PI = Preprocessing (Fpi)

 Fv = Perform Minutiae feature extraction (PI)

 From All Feature vector instance Fvi

 MDV_{fvi} = Estimate MDV (Fvi)

 End

 Compute MRMDV = $\frac{\sum MDV}{size(Fvs)}$

 With any feature vector of trained set

```

    Measure Minutiae Depth Similarity
MDS = Dist(MRMDV,MRMDV(ti)
End

Compute cumulative MDS CMDS =  $\frac{\sum MDS}{size(Ds)}$ 

If CMDS>Th, then
    Alert Altered print.
End
End
Stop
    
```

The multi-region minutiae depth measure-based approach computes the minutiae depth value on each region which is classified according to the threshold value towards altered fingerprint.

6. Experiments and results

The multi-region minutiae depth value-based altered fingerprint detection scheme is hard coded with Matlab Tool, and the performance of the method is evaluated on different parameters. The results obtained are presented in this section.

The experimental setup being used for the performance evaluation of the proposed MRMDV-based approach is shown in Table 1. The evaluation is conducted by measuring different performance metrics and discussed here. The analysis of liveness detection accuracy is presented in Fig 3.

The accuracy in liveness detection is measured for different methods and analyzed in Fig 3. The proposed MRMDV has achieved higher accuracy than other schemes.

$$False\ Detection\ Ratio = \frac{Number\ of\ false\ detetion}{Total\ number\ of\ samples} \times 100 \tag{1}$$

Average Classification Error(ACE) which is an averaged sum of APCER and BPCER. APCER and BPCER can be determined using the Eqs 2 and 3.

$$AP\ CER = \frac{Number\ of\ mis - classified\ fake\ samples}{Total\ fake\ samples} \times 100 \tag{2}$$

Table 1. Evaluation details.

Parameter	Value
Tools Used	Matlab
Users	500
Total fake prints	50

<https://doi.org/10.1371/journal.pone.0293249.t001>

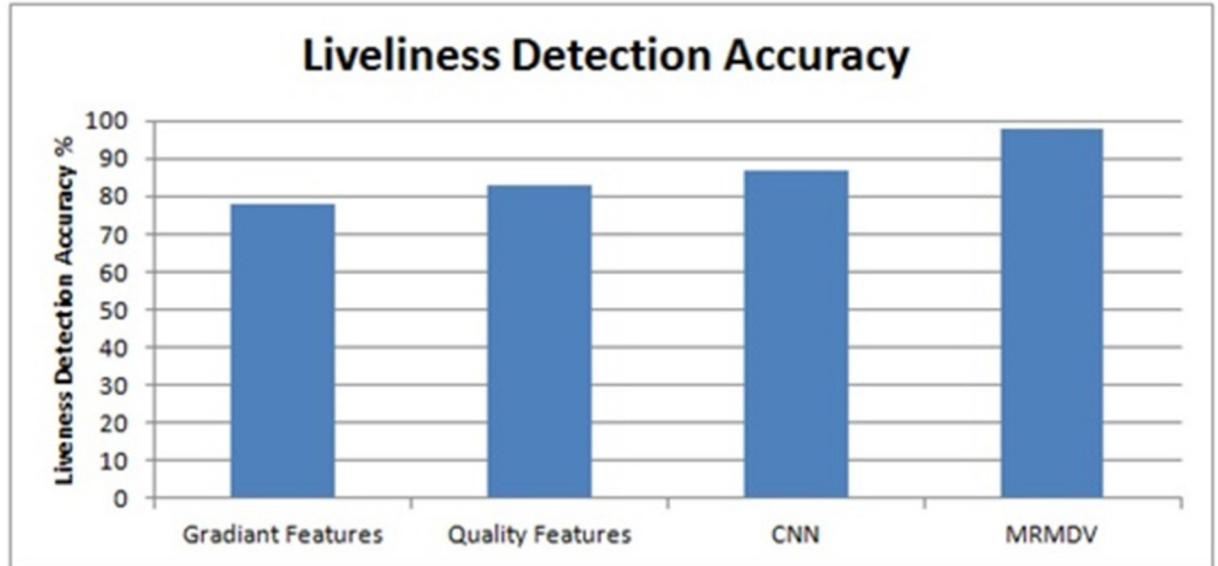


Fig 3. Analysis of liveliness detection accuracy.

<https://doi.org/10.1371/journal.pone.0293249.g003>

$$BPCER = \frac{\text{Number of mis - classified live samples}}{\text{Total live samples}} \times 100 \tag{3}$$

$$ACE = \frac{APCER + BPCER}{2} \tag{4}$$

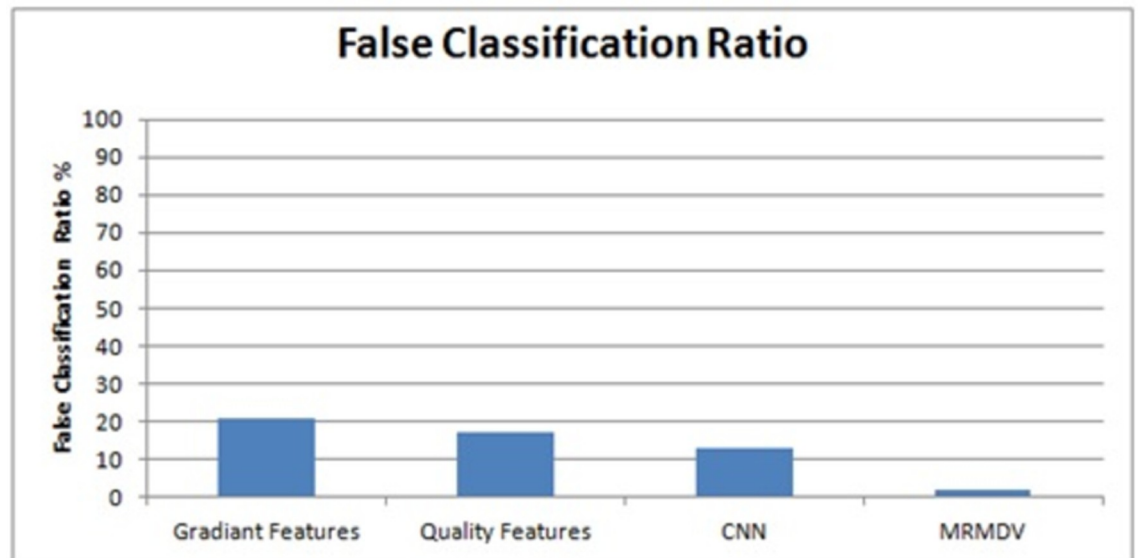


Fig 4. Analysis on false ratio.

<https://doi.org/10.1371/journal.pone.0293249.g004>

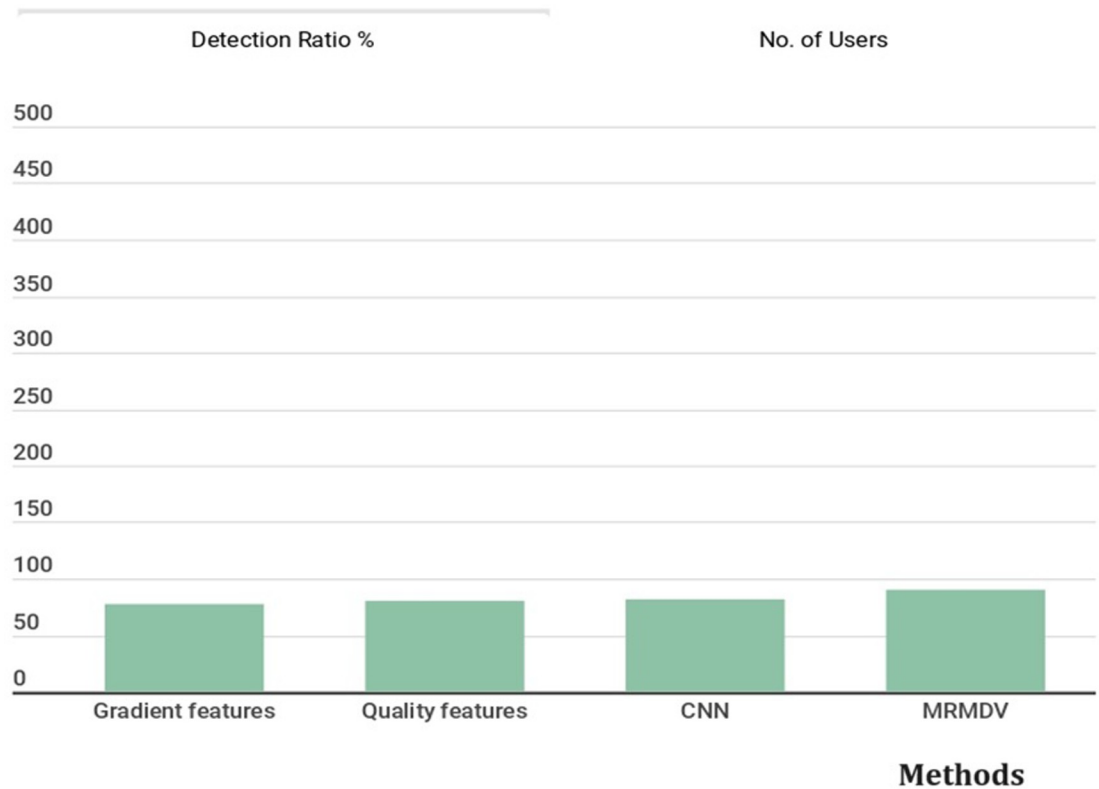


Fig 5. Detection ratio of the uniform users.

<https://doi.org/10.1371/journal.pone.0293249.g005>

The false ratios introduced by different approaches are plotted in Fig 4, where the MRMDV scheme reduces the false ratio. The detection ratio for the uniform users is presented in Fig 5. This provides detailed analysis of uniform users and its related methods.

The analysis of time complexity produced is as shown in Fig 6. The analysis of time complexity produced and its time complexity measures include various approaches is also presented Fig 6. This figure represents that the proposed MRMDV algorithm introduces less time complexity compared other existing methods considered in this research.

7. Discussion and conclusion

In this work, a multi-region minutiae depth based fingerprint analysis algorithm is presented. The input image has been fetched, and noise has been removed to improve the quality of the image. Further, a list of tiny images is cropped from the input image, and features of such tiny images are extracted. The features extracted have been used to measure the value of MRMDV. With the MRMDV value, the value of CMDS is measured to classify the fingerprint as forged or original. The MRMDV scheme achieves higher performance in detecting altered prints with the least time complexity and false ratio.

The proposed MRMDV model has certain limitations on the accuracy. The accuracy is depending on the volume of training set used. Also, the work can be extended by concerning the features like number of rises on edges and number of sharp edges present in the image towards measuring the similarity.

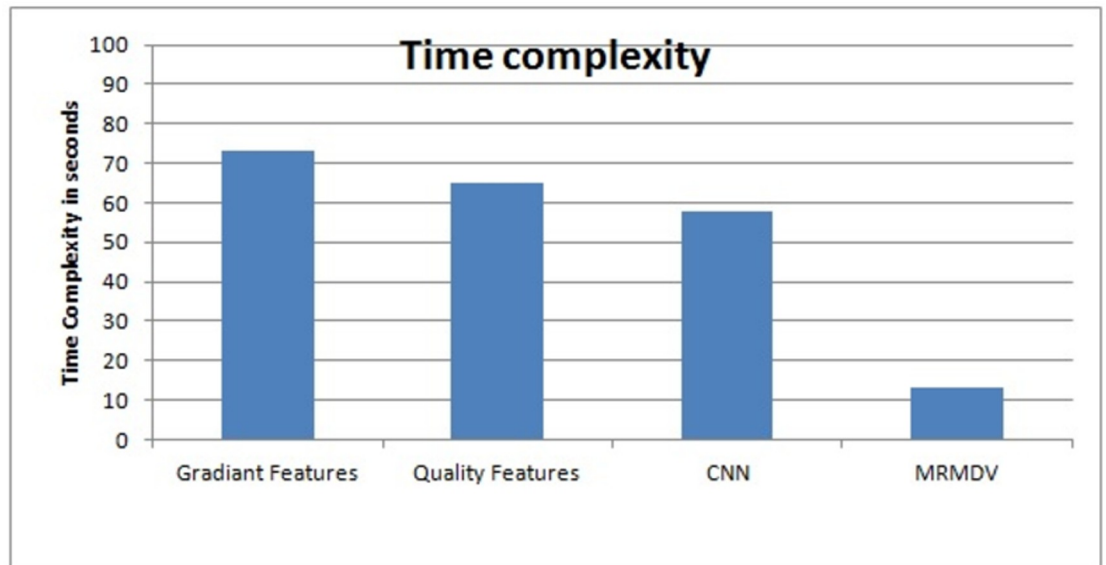


Fig 6. Analysis on time complexity.

<https://doi.org/10.1371/journal.pone.0293249.g006>

Supporting information

S1 File. Code for preprocessing and edge detection.
(DOCX)

Acknowledgments

The authors extend their appreciation to the Faculty of Management, Comenius University in Bratislava, Odbojárov 10, 82005 Bratislava 25, Slovakia for providing the funding for this Manuscript.

Author Contributions

Conceptualization: M. Baskar, Renuka Devi Rajagopal, PRASAD B. V. V. S., J. Chinna Babu.

Data curation: M. Baskar, J. Chinna Babu, Gabriela Pajtinková Bartáková, T. S. Arulananth.

Formal analysis: M. Baskar, Renuka Devi Rajagopal, PRASAD B. V. V. S.

Funding acquisition: Gabriela Pajtinková Bartáková.

Methodology: M. Baskar, Renuka Devi Rajagopal, PRASAD B. V. V. S.,
Gabriela Pajtinková Bartáková.

Supervision: J. Chinna Babu, Gabriela Pajtinková Bartáková, T. S. Arulananth.

Writing – original draft: M. Baskar.

Writing – review & editing: M. Baskar, Renuka Devi Rajagopal, T. S. Arulananth.

References

1. Josphineleela R. et al., A New Approach of Altered Fingerprints Detection on The Altered and Normal Fingerprint Database, Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No.6 Dec 2012-Jan 2013
2. Yoon Soweon Altered Fingerprints: Analysis and Detection, IEEE Transaction on software engineering, 34(3):451–64 · July 2011

3. MaciejSzymkowski; Khalid Saeed, A novel approach to fingerprint identification using method of sectorization, IEEE conference on, Biometrics and Kansei Engineering (ICBAKE), 2017
4. Rudolf Haraksim; Alexandre Anthonioz; Altered fingerprint detection—algorithm performance evaluation, IEEE Conferences on Biometrics and Forensics (IWBF), 2016
5. Serena Papi; Matteo Ferrara; On the Generation of Synthetic Fingerprint Alterations, Biometrics Special Interest Group (BIOSIG), 2016
6. Vinodhet A.. AI, An Analysis of Altered Fingerprint Detection, Recognition, and Verification, International Journal of Computer Science and Mobile Computing, Vol. 5 Issue.1, January- 2016, pg. 178–182
7. Selvarani S.; Jeba Priya S.; Smeeta Mary R., Automatic Identification and Detection of Altered Fingerprints, IEEE International conference on Intelligent Computing Applications (ICICA), 2014.
8. Sousedik Ctirad; Busch Christoph, Presentation attack detection methods for fingerprint recognition systems: a survey, IET Biometrics, Vol. 3(4), 2014.
9. Manikandan K.latha, Critical Analysis and Detection of Altered Fingerprints, International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014.
10. Asraf ul Syifaa Ahmad, Rohayanti Hassan, and Razib M. Othman, An investigation of fake fingerprint detection approaches, AIP Conference Proceedings, Volume 1891, Issue 1, 2017.
11. Xia Z., Lv R., Zhu Y., Ji P., Sun H., and Shi Y. Q., "Fingerprint liveness detection using gradient-based texture features," *Signal, Image Video Process.*, vol. 11, pp. 1–8, 2016.
12. Hadid A., Evans N., Marcel S., and Fierrez J., "Biometrics Systems Under Spoofing Attack: An evaluation methodology and lessons learned," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 20–30, 2015.
13. Park E., Kim W., Li Q., Kim H., and Kim J., "Fingerprint liveness detection using CNN features of random sample patches: Liveness detection using CNN features," *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, vol. P-260, 2016.
14. Arunalatha G. and Ezhilarasan M., "Fingerprint Spoof Detection Using Quality Features," *Int. J. Secur. Its Appl.*, vol. 9, no. 10, pp. 83–94, 2015.
15. Galbally J., Alonso-Fernandez F., Fierrez J., and Ortega-Garcia J., "A high-performance fingerprint liveness detection method based on quality related features," *Futur. Gener. Comput. Syst.*, vol. 28, no. 1, pp. 311–321, 2012.
16. Vinoth A. and Saravanakumar S., Accuracy Fingerprint Matching For Altered Fingerprint Using Divide And Conquer And Minutiae Matching Mechanism, *ARPN Journal of Engineering and Applied Sciences*, VOL. 11, NO. 21, 2016.
17. Moud M.H.Ali, Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching, IEEE International conference on Advanced Computing, 2016.
18. Pavithra R, Suresh K V, Fingerprint Image Identification for Crime Detection, IEEE International Conference on Community and Signal Processing, 2019.
19. Nuraisha Safira, Guruh fajar Shidik, Evaluation of Normalization in Fake Fingerprint Detection with Heterogeneous Sensor, International Conference on Application of technology on information and communication, 2018.
20. Diaan M Uliyan, Anti-spoofing method for fingerprint recognition using patch-based deep learning machine, Elsevier, International Journal of Engineering Science and Technology, (23) 2, pp: 264–273, 2020.
21. Baskar M., Renuka Devi R., Ramkumar J., Kalyanasundaram P., Suchithra M. & Amutha B., Region Centric Minutiae Propagation Measure Orient Forgery Detection with Finger Print Analysis in Health Care Systems. *Neural Processing Letters*, Vol. 55, pp.19–31, 2023.
22. Neil Zhenqiang Gong, Forgery-Resistant Touch-based Authentication on Mobile Devices, ACM, conference on computer and communication, 2016.
23. Fahmy M.F, Fahmy O.M, A new morphological based forgery detection scheme, IEEE, National Radio Science Conference, 2016.
24. Arulananth T. S. and Shilpa B., "Fingertip-based heartbeat monitoring system using embedded systems," 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2017, pp. 227–230, <https://doi.org/10.1109/ICECA.2017.8212802>
25. Arulananth T. S., Sujitha M., Nalini M., Srividya B. and Raviteja K., "Fake shadow detection using local histogram of oriented gradients (HOG) features," 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2017, pp. 739–742, <https://doi.org/10.1109/ICECA.2017.8212765>
26. Rajasekar V., Predić B., Saračević M., Elhoseny M., Karabasevic D., Stanujkic D., et al (2022), Enhanced Multimodal Biometric Recognition Approach for Smart Cities Based on an Optimized Fuzzy Genetic Algorithm, *NATURE Scientific Reports*, 12, Article number: 622.

27. Hassan R., Pepic S., Saračević M., Ahmad K., Tasic M. (2021), A Novel Approach to Data Encryption based on Matrix Computations, *CMC—Computers, Materials and Continua*, Tech Science Press, Vol. 66, No.2, pp.1139–1153.
28. Elsadai A., Adamović S., Šarac M., Saračević M., Kumar Sharma S. (2021), New Approach for Fingerprint Recognition Based on Stylometric Features with Blockchain and Cancellable Biometric Aspects, *Multimedia Tools and Applications*, 81, pages 36715–36733, <https://doi.org/10.1007/s11042-021-11581-w>.
29. Sharma B., & Aseri T. C. (2015). A hybrid and dynamic reliable transport protocol for wireless sensor networks. *Computers & Electrical Engineering*, 48, 298–311.
30. Gupta M., Kumar R., Shekhar S., Sharma B., Patel R. B., Jain S., et al. (2022). Game theory-based authentication framework to secure internet of vehicles with blockchain. *Sensors*, 22(14), 5119. <https://doi.org/10.3390/s22145119> PMID: 35890796
31. Kharb K., Sharma B., & Trilok C. A. (2016). Reliable and congestion control protocols for wireless sensor networks. *International Journal of Engineering and Technology Innovation*, 6(1), 68.
32. Koundal D., & Sharma B. (2019). Challenges and future directions in neutrosophic set-based medical image analysis. In *Neutrosophic Set in Medical Image Analysis* (pp. 313–343). Academic Press.