Region based Minutiae Mass Measure for Efficient Finger Print Forgery Detection in Health Care System

A. Vinoth, S. Saravanakumar

Abstract: ***The modern security system has used various biometrics in authenticating the human. Among them, the finger print has been used as the key in major systems. Even though, the finger prints are unique and cannot be modified, there are intrusions which are performed by fake finger prints prepared by malicious entities. 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. Then the noise removed image has been improved for its quality by sharpening the edges of ridges present in the image. Then the image has been split into number of regions and for each sectional image, the method extracts various minutiae features like ridge island, number of ridge dots, ridge ends, ridge enclosures, and ridge bifurcation. Using the features extracted, the method estimates the Minutiae mass value for each sectional image. 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.***

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 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.

Revised Manuscript Received on December 30, 2018.

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 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.

Figure 1: Sample Altered Finger Prints

The Figure 1, shows the sample genuine finger prints and altered one. In first finger print, there are additional edges created and the second image has altered with enclosures and curve being tilted.

The malicious users would generate fake finger prints to intrude the security systems. In any finger print, it characteristics like minutiae can be identified. The minutiae is the ridge and there are number of ridge characteristics present in the finger print namely ridge island, dots, end, enclosures and bifurcation. 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 WORKS

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 (fully-implemented) 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.

Biometric Fingerprint System to Enable Rapid and Accurate Identification of Beneficiaries [18], founded SimPrints, a nonprofit health technology organization centered on development of a pocket-sized fingerprint scanner that wirelessly syncs with a health worker's smartphone to link individuals' fingerprints to their health records.

Fingerprint and Iris Template Protection for Health Information System Access and Security [19], focus on template database attacks which includes attacks on the integrity of biometric templates by presenting a new approach using both chaos and Hadamard matrices. Although a considerable amount of work was conducted on protecting biometric templates, the proposed approaches in the literature do not satisfy the main requirements of security, performance, diversity and revocability. However, our approach contributes better results in case of recognition rate i.e., 100 percent, zero percent false rejection rate and false acceptance rate and satisfies the requirements of revocability, diversity and privacy.

In [20], combination of biometrics and other personal identification techniques were used to identify individual's resident within a surveillance population seeking care in two district hospitals. Visits from resident individuals were successfully recorded and categorized by the success of the techniques applied during identification. The successes of visits that involved identification by fingerprint were further examined by age.

All the above discussed methods suffer to achieve higher performance in forgery detection and requires some strategically approach.

III. MMM BASED ALTERED 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.

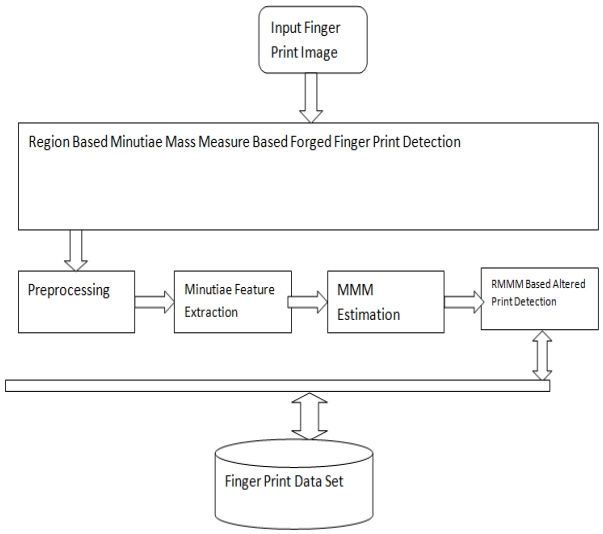

Figure 2: Architecture of Proposed RMMM Based Forged Finger Print Detection System

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 = $\int_{i=1}^{Nos}$ split(EI, $< Sa, Ea >$
Nos – no of sections or regions
Sa – Starting angle
Ea- Ending angle.
For each sectional image Si
Extract Minutiae island Mi = $\sum$ Islands $\in$ Si
Extract Minutiae dots Md = $\sum$ Dots $\in$ Si
Extract Minutiae End Me = $\sum$ End $\in$ Si
Extract Minutiae enclosures Men = $\sum$ Enclosures $\in$ Si
Extract Minutiae Bifurcation Mb = $\sum$ Bifurcation $\in$ Si
Construct feature vector Fvi = {Mi, Md,Me, Men, Mb}
Add to feature vector Fv = $\sum$(Fvk $\in$ Fv) $\cup$ Fvi
End
Stop

The feature extraction algorithm extracts various features from each sectional image and add to the feature vector.

Generated feature vector has been used to estimate MMM measure in the next stage.

MMM Estimation

The MMM measure represent the mass value of ridge feature computed based on the ridge feature being extracted. To estimate the MMM value, the number of dots, edge, bifurcation, end and enclosures are computed. Based on that, the mass value of each measure has been estimated. This will be measured for each regional or sectional image based on the feature vector given. Using all the values, the MMM value has been measured. The estimated MMM value has been used to classify the input finger print image.

Algorithm

Input: Feature Vector Fv
Output: MMM
Start
Read Feature vector Fv.
Compute Number of dots present Nod = $\int_{i=1}^{size\ (Fv)} \sum Fv.Minutiae == dot$
Compute No of Edge NoE = $\int_{i=1}^{size\ (Fv)} \sum Fv.Minutiae == edge$
Compute no of ends Noed = $\int_{i=1}^{size\ (Fv)} \sum Fv.Minutiae == end$
Compute no of enclosures Noen = $\int_{i=1}^{size\ (Fv)} \sum Fv.Minutiae == enclosure$
Compute No of bifurcation Nob = $\int_{i=1}^{size\ (Fv)} \sum Fv.Minutiae == Bifurcation$
Compute Minute Mass Mm = $\frac{Noen}{size\ (SI)} \times \frac{Nod}{Noe} \times \frac{Noed}{Nob}$
Compute cumulative Minute Mass Measure MMM = $\frac{\sum MM}{size\ (Fv)}$
Stop

The above discussed algorithm computes the minutiae mass measure value based on the features of the minutiae and would be used to perform classification.

RMMM Based Altered Finger Print Detection

The forged finger print or articulated finger print has been classified based on the minutiae mass measure estimated on a given image The input image has been read and preprocessed to remove the noise and enhance the image. The enhanced image has been split into number of sectional image and for each sectional image, the method extracts various features from the sectional image. Using the features extracted, the method computes the minutiae mass measure on each regional image. Based on estimated measures, the method computes the similarity with the various feature set available. Based on the similarity threshold, the method classifies the finger print as natural or articulated.

Algorithm

Input: Finger print image Fpi, Data set Ds.
Output: Boolean
Start
Read Input image Fpi
Read data set Ds.
PI = Proprocessing(Fpi)
Fv = Minutiae feature extraction (PI)
For each feature Fvi
MMM_{fvi} = Estimate MMM(Fvi)
For each feature Fvd from data set
MMM_{fvd} =Compute MMM (Fvd)
End
Compute cumulative MMM = $\frac{\sum MMM}{size\ (Ds)}$
Compute similarity of both the values.
SimDist = Dist(MMM_{fvi} , MMM_{fvd})
If SimDist>SimTh then
Forged and return false
End
End
Stop

The above discussed algorithm computes the minutiae mass measure on each region and based on the threshold value the forged region or forged print has been identified.

IV. RESULTS 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.

Table 1: Details of Evaluation

Parameter	Value
Tool Used	Matlab
No of classes	500
No of fake prints	50

The Table 1 shows the details of evaluation being used to measure the performance of the proposed algorithm. The method has been evaluated with the finger prints of five hundred persons. For the classification, there are 50 fake finger prints has been considered. The proposed method has produced the following results.

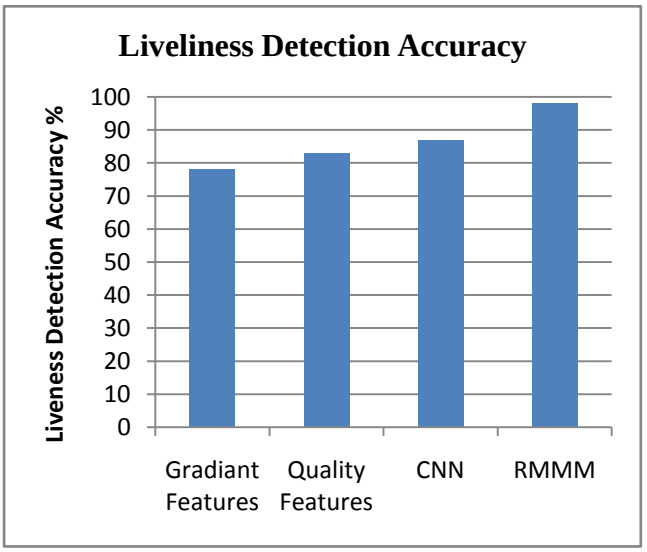

Figure 4: Comparison on Liveliness Detection Accuracy

The Figure 4, shows the comparative result on liveliness detection accuracy produced by various approaches. The proposed algorithm has improved the performance of liveliness detection accuracy than other methods.

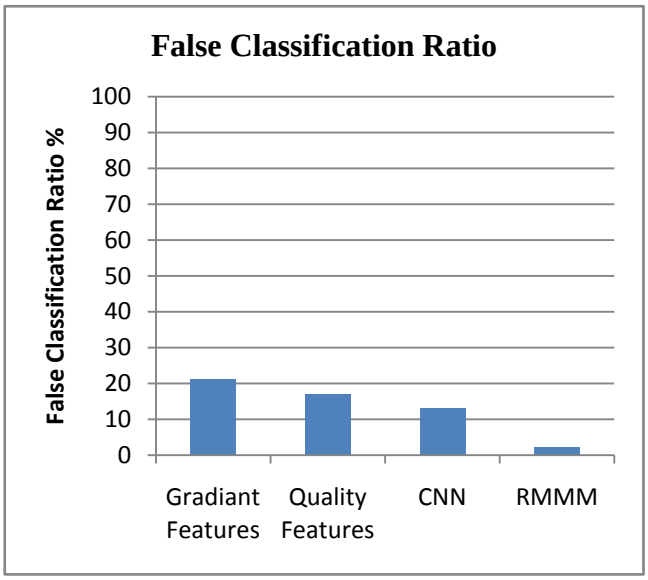

Figure 3: Comparison on False Classification Ratio

The Figure 3, shows the comparison result on false classification ratio produced by various methods and the proposed algorithm has produced less false ratio compare to other methods.

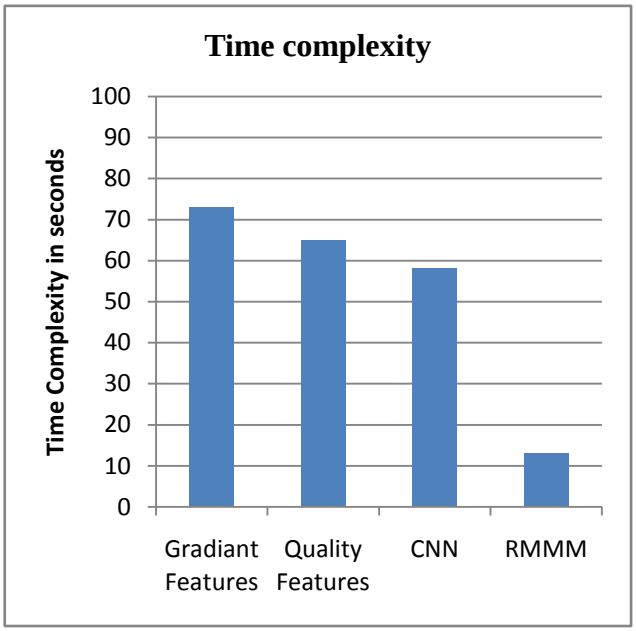

Figure 5: Comparison on Time Complexity

The Figure 5, shows the comparative result on time complexity produced by different methods and the result shows that the proposed method has produced less time complexity than other methods.

V. CONCLUSION

In this paper an efficient region based altered finger print 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. R.Josphineleela 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. Soweon Yoon Altered Fingerprints: Analysis and Detection, IEEE Transaction on software engineering, 34(3):451-64 · July 2011
3. Maciej Szymkowski ; 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. A.Vinoth et. Al, 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. S. Selvarani ; S. Jebapriya ; R. Smeeta Mary, Automatic Identification and Detection of Altered Fingerprints , IEEE International conference on Intelligent Computing Applications (ICICA), 2014.
8. Ctirad Sousedik ; Christoph Busch, Presentation attack detection methods for fingerprint recognition systems: a survey, IET Biometrics (Volume: 3, Issue: 4, 12 2014)
9. K.latha, Manikandan, 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. Asraful Syifaa' Ahmad, Rohayanti Hassan, and Razib M. Othman, An investigation of fake fingerprint detection approaches, AIP Conference Proceedings, Volume 1891, Issue 1, 2017.
11. Z. Xia, R. Lv, Y. Zhu, P. Ji, H. Sun, and Y. Q. Shi, "Fingerprint liveness detection using gradient-based texture features," Signal, Image Video Process., vol. 11, pp. 1–8, 2016.
12. A. Hadid, N. Evans, S. Marcel, and J. Fierrez, "Biometrics Systems Under Spoofing Attack: An evaluation methodology and lessons learned," IEEE Signal Process. Mag., vol. 32, no. 5, pp. 20–30, 2015.
13. E. Park, W. Kim, Q. Li, H. Kim, and J. Kim, "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. G. Arunalatha and M. Ezhilarasan, "Fingerprint Spoof Detection Using Quality Features," Int. J. Secur. Its Appl., vol. 9, no. 10, pp. 83–94, 2015.
15. J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "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. A.Vinoth and S.Saravanakumar, 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. Alyssa Iacona,Health Care Information Technology: Securing the Electronic Health Record with Biometric Technology, A journal of undergraduate student research, vol.15, issue 4, 2018.

18. Daniel Matthew L Storisteanu, Toby L Norman, Alexandra Grigore and Tristram L Norman, Biometric Fingerprint System to Enable Rapid and Accurate Identification of Beneficiaries,Global health science and practices, vol 3, issue 1, 2015.
19. Abdul, Wadood, Alzamil, Abdullah,Fingerprint and Iris Template Protection for Health Information System Access and Security, Journal of Medical Imaging and Health Informatics, Volume 7, Number 6, 2018.
20. Eliezer Ofori Odei-Lartey, The application of a biometric identification technique for linking community and hospital data in rural Ghana, Global health action, 2016.