A PROPOSED SCHEME FOR FINGERPRINT RECOGNITION SYSTEM USING BOZORTH3 ALGORITHM

[1]Sandesh Zanwar, [2]Priyanka Nangare, [3]Vaibhav Supe, [4]Jayaprabha Yadav
[1,2,3,4]P.E.S Modern College Of Engineering

Abstract— Minutiae, those irregularities in the ridges on a finger of a person are rich in details, are unique to every individual. Thus, extraction of biometric pattern of these minutiae from sample data of fingerprint forms the prime task in formation of automatic fingerprint recognition system. To authenticate a person's identity a NIST reference system is used for matching minutiae patterns on a finger. It starts with binarization of each grayscale input image for locating minutiae points. Then a finger print matcher, using a digital image processing compares input search with all available data samples to make a conclusion of most probable existing match. No subject will be required to carry hard documents with this recognition system being in usage. Technological advancement towards mobile and handheld devices like tablets will only promote this mechanism. The proposed work envisages a process of paperless documentation using superlative features of android application developments and concepts like multithreading for thumb recognition simplifying tedious tasks similar to that of governments'

Index Terms—Biometrics, BOZORTH3, NIST, Thumb Recognition

I. INTRODUCTION

All over India traffic police use hard documents to verify persons' identity. This proves to be a herculean task for people as well as the verification officers. Considering the user public prospective there is a need of paperless documentation which isn't catered by RTOs in India. The persistent issue people experience is the tedious task of carrying hard copied documents which also implies probability of information loss over a span of time.

The finger print recognition technique is based on recognition, differentiation and matching of distinctive characteristics of a fingerprint. A finger print recognition device collates finger print image data; For the process of extraction of unique features Bozorth3 algorithm is put to application. As and when the match is located officers will get all the detailed information about vehicle on synchronized handheld android device. Now a day's android technology is available with almost everyone, this technology will not only save time involved in verification process but also will be cost effective.

This proposed work serves a solution for detection of network attacks such as Distributed Denial of Service attack in a Software Defined Network using Support Vector Machine and Entropy based discretization algorithms. The main objective of the proposed work is to identify the identity, authority and regulation towards on road drivers in India. Thus, the proposed application will not only reduce the tasks involved in RTOs but will also make documentation paperless.

II. PREVIOUSLY WORK DONE

In paper [1], present partial fingerprint problem as quality issue is addressed. Performance of the fingerprint recognition system heavily depends on the quality of the fingerprint image. In paper [2], the NIST reference system uses minutiae based matcher to authenticate a person's identity. Firstly, the minutiae detection algorithm relies on binarization of each gray scale input image in order to locate all minutia points (ridge ending and bifurcation). Then, the matching algorithm computes a match score between the minutia pairs from any two fingerprints using the location and orientation of the minutiae points. The matching algorithm is rotation and translation invariant. Finally, the two fingerprints are from the same finger when the match score is higher than a threshold. The algorithm proposed in this paper solve every optimization problem that is the problem of finding the best solution from all feasible solutions. The paper [3] discusses on the standardized fingerprint model which is used to synthesize the template of fingerprints.

The paper [4] is a study and implementation of a fingerprint recognition system based on Minutiae based matching quite frequently used in various fingerprint algorithms and techniques. The proposed approach mainly involves extraction of minutiae points from the sample fingerprint images and then performing fingerprint matching based on the number of minutiae pairings among two fingerprints in question. The proposed system in this paper mainly incorporates image enhancement, image segmentation, feature (minutiae) extraction and minutiae matching. As a result, it generates a percent score which tells whether two fingerprints match or not. In paper [5], the differences between real and fake fingerprints as the first step to approach the problem is discussed. The effects of different imaging sensors on the sizes of templates and on the matching scores between real and fake fingerprints is studied in this paper. In paper [6], the first scalable, efficient, and reliable privacy-preserving minutiae based fingerprint authentication is presented.

III. PROPOSED SYSTEM ARCHITECTURE

Following fig shows the system architecture of proposed system:

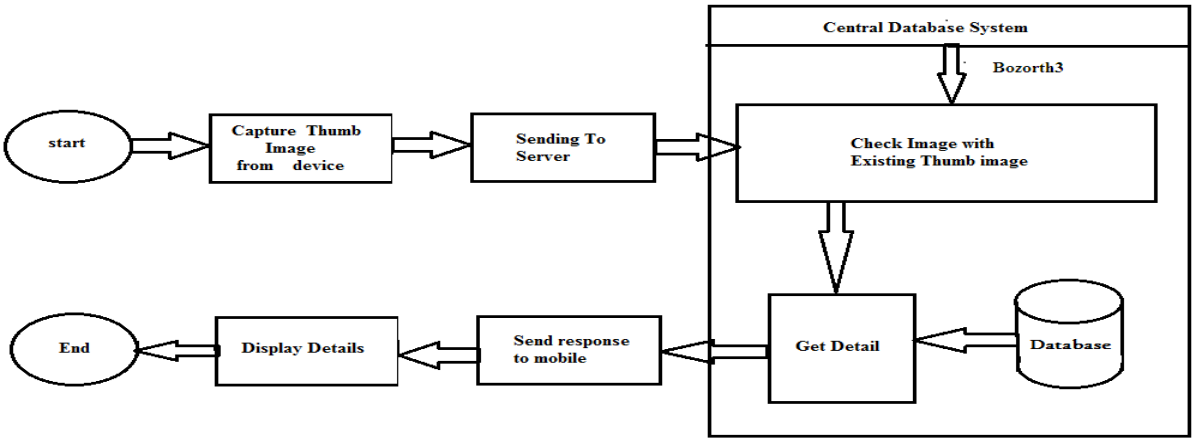

Fig 3.1 System Architecture

The proposed system is mainly divided into two modules i.e. User module and Application module. In user module, after successful login of user the application is activated for that user. The thumb impression of driver is captured using thumb recognition device by the traffic police. The captured thumb impression is sent to the server. In the application module, the match score of the thumb impression will be calculated and the details of the corresponding user fetched from the database will be sent to the android application. Fine calculation and deduction will be automatically handled by the proposed system. The following steps the overall flow of the proposed system.

1. The system will accept the fingerprint through the thumb recognition device.
2. In the central database using Bozorth3 algorithm the image is matched with the images in the database with the match score.
3. If the match score is above the threshold then details of the respective image are sent to the mobile as a response.
4. The details are displayed on the screen of android application.
5. The system will automatically deduct fine from the person's bank account.
6. The system will only verify the person's document and not issue any documents from the RTO.

IV. BOZORTH3 ALGORITHM

The BOZORTH3 module computes a match score between the pairs of minutiae from any two fingerprints. Three key things are important about this fingerprint matcher: A] It is only based on the location and orientation of the minutiae points. B] Only the 150 highest-quality minutiae are used. C] The algorithm is designed to be rotation and translation invariant.

The algorithm is comprised of three major steps:

1. Construct intra-fingerprint minutia comparison tables:
The first step in the bozorth3 matcher is to compute relative measurements from each minutia in a fingerprint to all other minutia in the same fingerprint. These invariant measurements are distance between two minutiae and angle between each minutia's orientation and the intervening line between both minutiae. These measurements are then stored in a minutia comparison table (for the matching step, there will be one table for the enrolment fingerprint and one table for the test fingerprint to be matched against).

2. Construct an inter-fingerprint compatibility table:
The second step in the bozorth3 matcher is to take the intra-fingerprint minutia comparison tables from the two fingerprints (enrolment and test) and look for compatible entries between the two tables. Table entries are considered to be compatible if the corresponding distances and the relative minutiae angles are within a specified tolerance. An inter-fingerprint compatibility table is then generated, only including entries that are compatible.

3. Traverse the inter-fingerprint compatibility table:
The final step of the matcher consists in traversing and linking table entries into clusters, combining compatible clusters and accumulating a match score. The larger the number of linked compatibility associations, the higher the match score, and the more likely the two fingerprints are from the same person.

V. CONCLUSION

Unlike traditional fingerprint recognition system takes more time for recognition because of pre-processing and post processing of images which becomes impractical; the proposed system implementation is an effort to understand how Fingerprint Recognition could be used as a biometric recognition mechanism to identify users. It encompasses all the steps from minutiae extraction to matching of them which in turn generates a match score. The promised mobility, centralized control for RTO process using the biometric thumb capture technology are prominent features of proposed application.

REFERENCES

[1] Ishan Khurjekar, Bhushan Garware, Aditya Abhyankar," Towards Minimizing Effect of Partial Fingerprint Images on the Performance of Fingerprint Recognition Systems", IEEE 2015.
[2] Aurelien Mayoue," A biometric reference system for fingerprint NIST Fingerprint Image Software", Biosecure 2008.
[3] Abhishek Nagar, Heeseung Choi, Anil K. Jain," Evidential Value of Automated Latent Fingerprint Comparison:An Empirical Approach", IEEE 2012.
[4] Sangram Bana, Dr. Davinder Kaur," Fingerprint Recognition using Image Segmentation", IJAEST 2011.
[5] Qinghai Gao,"A Preliminary Study of Fake Fingerprints", IEEE 2014.
[6] Ye Zhang," Robust PrivacyPreserving Fingerprint Authentication", IEEE 2015.