LICENCE MANAGEMENT SYSTEM USING ANDROID BASED MOBILE BIOMETRICS

Narayanan Ramakrishnan[1], Shradhaa Parkar[2], P.B. Vijayalakshmi[3]

[1,2]UG Scholar, [3]Assistant Professor,Computer Engineering,

Fr. C. Rodrigues Institute of Technology, Vashi, Maharashtra, (India)

ABSTRACT

Mobile based bio-metrics employing android technology provides an important front-line security in every domain. Based around a central biometric identification system (BIS), mobile based biometrics extend the functionality and capabilities of a static BIS by allowing users to capture fingerprints out in the field, and compare minutiae against remotely stored bio-metric databases. The idea of our project is to develop a client server android application, capturing the images of number plate of the driver's vehicle and the driver's fingerprints, upon which OCR and BOZORTH3 algorithms being performed respectively. For a match, the corresponding records being fetched from the database consisting of personal details, licence details, vehicle information. A track of history of numerous offenses would be kept at server side and updated continuously by the officials in the field. Also, in case of vehicles not complying with their registered users, an SMS would be sent being integrated with the application to instantly check for malicious vehicle thefts. Additionally, data mining using analytics is done on offenses info for determining any subtle statistical patterns of drivers and keeping a check on the road-side menaces.

Keywords: Bio-metrics, BOZORTH, licence, MINDTCT, Minutiae, OCR.

I. INTRODUCTION

Bio-metrics encompasses a range of for identity verification [17] using speciality-traits in them. Bio-metrics main focus is to exploit those distinctive and eccentric features using them for recognizing one sample from the other. Bio-metric technologies[4] are slowly evolving [16]to become one of the most far-reaching and paramount factors[5] in recognition and identifying processes .With the proliferating and swelling cases revealing the shaky and fragile security system, it is imminent that the time is drawing near for a better, safe, secure, well-guarded biometric identification systems especially fingerprints [14].Additionally, Android is becoming far more outreaching with its cutting-edge technology[20] and sophisticated features. It is evident that these systems are roaring in the market and will hold a key factor in security systems. Bio-metric based android solutions provide authenticity to data additionally to transactions and other covert channels. The applications of mobile biometrics employing android varies from as common as fast food centres and banks to as far-reaching [5]as in military and clandestine purposes [1]to bio-metric residence permits[12],[13]. Numerous domains are embracing these technologies. The most eloquent and compelling characteristics of fingerprint scanning are their resolution and their elegant act of handling the fingerprint images. The questions posed to the reader are thus:-

1. So why not employ this strategy for curbing the menacing problems encountered during road travels due to licenses, drunk driving and other related cases?

2. At a staggering estimated 7.5Billion$ industry worldwide in 2014, aren't vehicle thefts a menace not only to officials, but also to the common-men?

Many surveys have estimated that majority of all drunken driving, rash and other notorious activities takes place with drivers who do not have a valid driving licence. Unlicensed [3] and underage driving has also been on a rise [3]. Additionally, Vehicle thefts occur every 40sec added by insurance costs soaring at several billion$. In Mumbai alone, 18000 vehicles are stolen out of 150000 in 2014. Alas, even traffic officials dealing with cumbersome paperwork and receipts [6] leads to even greater misery. A client server android application curbing these menaces and offering a solution *for the officials, with the officials* is the whole objective in this paper. A very general block diagram is as shown in Fig 1.

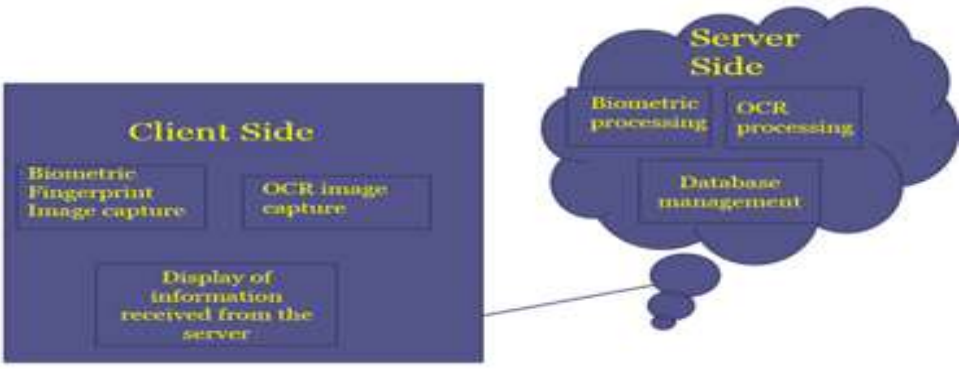

Fig. 1 Block Diagram of the Client and Server Side BIS.

II. OVERVIEW OF THE SYSTEM

The compelling characteristics providing an insight into the aspects of fingerprint biometrics are speciality-traits, accuracy and stability[2]. These form the main basis for further and detailed analysis. The steps involved in the whole process are:-

2.1 Wireless Access Using Socket Programming

Using IP address of the server, the login is made successful using socket programming. It requires an ad-hoc wireless network for fast fingerprint image transfer between the client and the server.

2.2 Peripheral Scanner

The peripheral device used is USB Fingerprint scanner: Nitgen Hamster DX for authentication, identification and verification functions[11]. The model used is HFDU-06[10] having technical specifications of 5V, 120 mA.

2.3 Procedure of Sensing

The classical and customary "ink and paper" method [11]was highly cumbersome. In the more popular live-scan method [11], the digitized image is gained by setting the thumb on the scanner. The process consists of acquiring the fingerprint image from the fingerprint scanner. Once the image is acquired, it is transferred to the Android Tablet used supporting OTG connectivity. Once the image is transferred to the tablet, it is then transferred to the server for further processing. The tablet should have two important features: one, it should possess a driving capability of equal or more than the scanner and two, it should possess the

"OTG"(On the Go) connectivity.

2.4 Phases of Usage

The different phases [15] involving system are:-

2.4.1 Enrolment Phase

During this phase, the scanner scans the driver's fingerprint and converts it into a digital image. The subtle distinctive points (ridge endings and bifurcations) are then extracted using MINDTCT and based upon this information, they stored into a file(stored template) used for further processing using BOZORTH3 algorithm explained later.

2.4.2 Corroboration Phase

In this phase, once the user touches the same sensor, generating a new fingerprint image called a test template [11].This then generates numerous minutiae files, and the matching module compares it with the stored minutia template (single template only) in the enrolment database.

2.4.3 Discerning Phase

In this phase, if the test fingerprint when matched with the stored templates generates a matching score above an optimal one, it is then considered to be the expected result and further processing commences verification as shown in Fig.2.

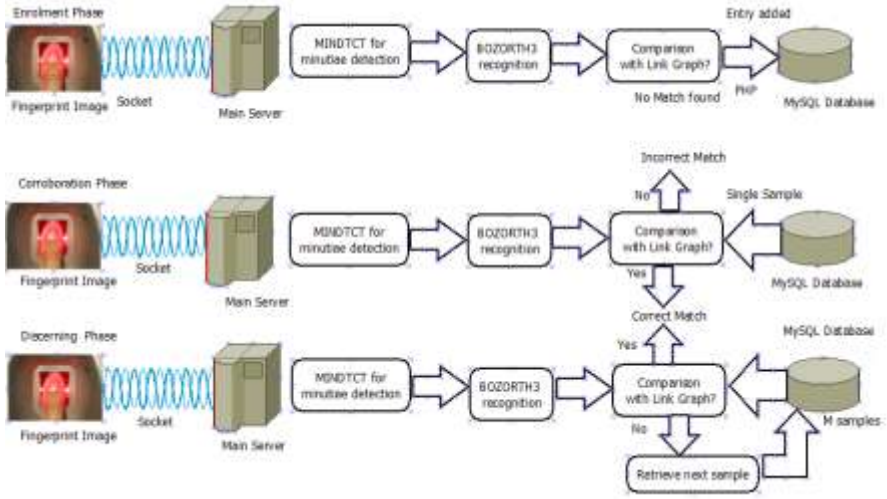

Fig. 2 Phases of Usages.

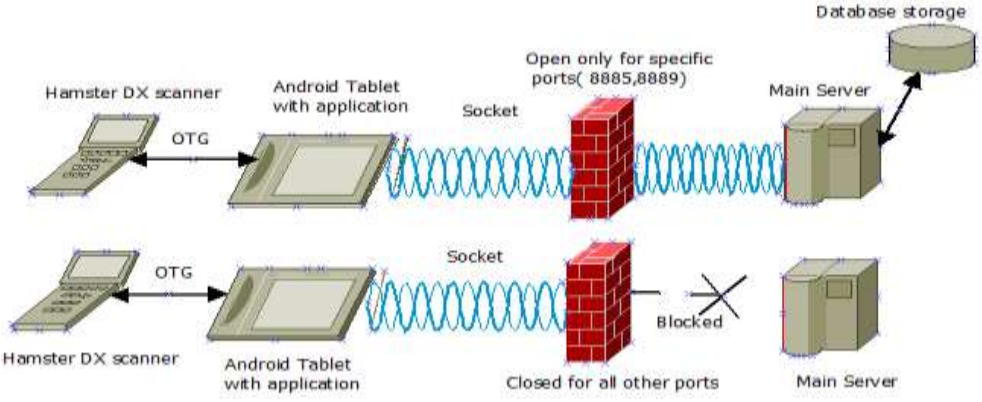

Fig.3 Process of Sensing Via the Tablet to the Remote Server

2.5 Fingerprint Processing Using Cygwin

Cygwin distribution provides numerous packages [19] of popular GNU tools and other headers, libraries for building and porting of applications. Following is the work of Cygwin for performing fingerprint processing:-

2.5.1 Mindtct

It was developed and still used by FBI's Universal Latent Workstation [14] which stands for "Minutiae Detection". For a given fingerprint image, [8]it determines the parameters necessary for further deduction which are location, orientation, quality and type. It uses these values for uniquely identifying the numerous fingerprints from the available samples found in the file folders in the main server. Minutiae are those specificities or the distinctive points which distinguish the sample points. Detection of these points thus forms one of the most important directive steps in the phase of fingerprint processing.

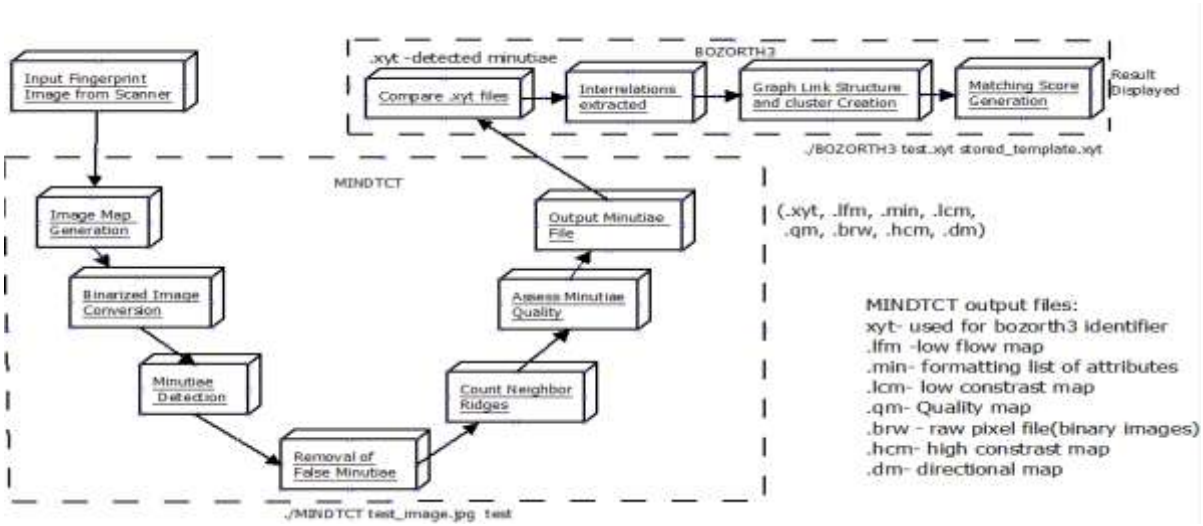

Fig.4 MINDTCT and BOZORTH3 operation

Command: ./MINDTCT [-b] <img_name> <oroot>S 1

As shown in (1); -b means image enhancement on low constrast images (optional). Image name means input name of the fingerprint image for processing. Lastly, "oroot" [21] signifies file name of the destination. Once the test image (in JPEG form only and if not, to be converted) is obtained in digitized form, it is subjected to various transformations [14] ,[18]collectively termed as MINDTCT involving:-

2.5.1.1 Image Map Transformation

This involves determining the parameters in the digitized images. These will form the initial basis for distinguishing different samples based on their subtleties.

2.5.1.2 Binary Image Conversion

All digitized images are converted to a Bi (2 level) images for further processing. Images having either high or low level can be subjected to extensive modifications.

2.5.1.3 Minutiae Detection

This phase deals with ridge endings and bifurcations. Each of the samples though similar to naked eyes have their own unique traits which are obtained in this phase.

2.5.1.4 Removal of False Minutiae

It is a very important stage to reduce FMR and others [20]. It involves removing islands, lakes, hooks and minutiae points too wide or too narrow (pores). It is similar to the noise removal in signal processing.

2.5.1.5 Count Neighbour Ridges

The resultant ridge-endings & curvatures are then counted to give a total for each of the samples.

2.5.1.6 Assess Minutiae Quality

This is determined by NFIQ discussed below describing a range of quality guideline numbers.

2.5.1.7 Output Minutiae File

These are the .extension files that are created. Out of these, .xyt containing the position(x, y coordinates), theta and orientation is further used for bozorth3 processing.

2.5.2 Nfiq

It determines the quality of the stored fingerprint images by using .qm (Quality Map) file. It gives output[18]as a series of numbers ranging from 1-5 where :1-Highest Quality 5-Lowest Quality as shown in (2).

Command: ./NFIQ <image_name> 2

2.5.3 Bozorth3

It is written by Alan. S. Bozorth at FBI [18]. The bozorth3 is on basis of minutiae for the matching algorithm and uses with regard to a matching score [14] for the different specific or subtle points and thus differentiates each and every sample by their location, quality, orientation and type. It is rotation and translation invariant [8]. It consists of two different tables for the fingerprint samples known as an Intra-fingerprint Specifics Differentiation Tables (ISDT), a Inter-fingerprint Similarity table (IST) for checking the matches and matching or suiting score(MS) using the IST. This algorithm can be described by the following steps which are:-

2.5.3.1 Isdt's

In this, we determine the relative measurements from one subtle point to all the other known specific (minutiae) points for both the test and stored template sample. By relative measurements, it both means distance and orientation between two minutiae points. The obtained results are stored in the ISDT's.

2.5.3.2 Ist

When the ISDT is created, a IST is created utilizing the parameters in ISDT for each of the two fingerprint samples. IST possesses those "consistent entries" which are "well-matched" entries between the two tables, each for the test and template. By consistent; it means that the matched measurements should be in justifiable forbearance. Basically, the IST holds the entries having very similar interrelations represented as single links in a graph- like structure.

2.5.3.3 Matching Score/Ms

Only and only if the matching score generated is high, will an entry be recorded in the database. The matching algorithm tries to amass all the sets of similar sampled table data entries via traversal into a large interrelated set of samples called as bunch. Thus greater the interrelations among the various bunches, greater the possibility of similarity and greater the MS.

Command: ./BOZORTH3 –A oufmt=sgp –g test.xyt template.xyt 3

The option –A outfmy-sgp displays the two minutiae parameter files to be compared and is optional as shown in (3).

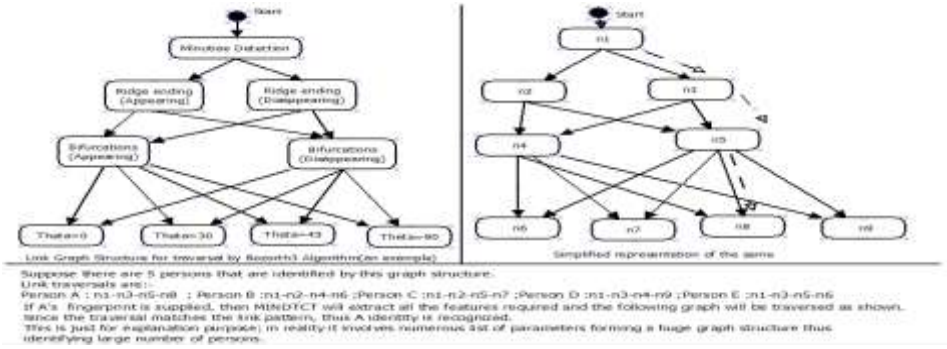

Fig. 5 Bozorth3 Description of Its Working

2.6 Optical Recognition Algorithm

A typical OCR system [9] consists of several components which are optical scanning, segmentation[7], pre-processing, feature extraction and post-processing as illustrated in Fig.6 shown below.

Fig.6 OCR Processing Description

2.7 Database Using MySQL and PHP on Xampp

Once the processing in Cygwin and OCR in Matlab is completed, for a particular match, the corresponding identifier is thrown which is captured and further used for retrieving the tuples in the database. There are 4 different databases namely: Personal_Info, Licence_Info, Vehicle_Info and Offenses.

Personal_Info: ID, PhoneNo, DOB, PhotoImage, Name

Licence_Info: LicenceNo, IssueDate, ExpiryDate, PlaceOfAuth

Vehicle_Info: NumberPlate, Colour, Type, DateOfReg.

Offenses: Name, typeOff, Location, Fine, Date, LicenceNo, Age.

These tables are updated continuously by the admin or some attributes selectively by the users through user interface developed. Due to fingerprint processing, Personal and licence details are retrieved. Due to OCR processing, Vehicle information is retrieved. Based upon the details, offenses are registered. A separate database is kept for number plates which are of 3 types:-

2.7.1 White List

These are the set of registered cars with the corresponding number plates and rightful owners.

2.7.2 Black List

These are the set of stolen cars with their number plates.

2.7.3 Grey List

These are the set of unregistered or unknown vehicle numbers.

2.8 SMS application

There arise two cases which are:-

2.8.1 Driver has reported the vehicle theft

In that case, the driver when reported instantly can be added to the black list. Additional details are also available in the list helping to nab thefts quickly.

2.8.2 Driver Has Not Reported or Unknown of the Theft

In that case, the driver is sent a SMS on his phone/phones to which instantly acknowledgement can be received and thus clarifications are received. Multiple phone numbers will be stored to facilitate the ongoing process. It will also benefit in better reliability in the system and more fault tolerance is achieved.

2.9 How numerous offenses are averted?

When powered with the system processing and android application on the device, this application provides a solution to the following problems:-

2.9.1 No Licence

If the driver caught at road without a licence faces a hefty fine otherwise, but with the application, it is averted.

2.9.2 Vehicle Thefts

A major hurdle is to determine whether a person has borrowed or stolen. It is determined by sending SMS to the specified owner of the vehicle and getting proper notification.

2.9.3 Others

Includes underage driving, unregistered vehicle, no helmet, no seatbelt, mobile driving, rash driving, no park violation, no horn violation, zebra crossing violation, signal break, roadside urination, wrong-side overtake ,no light after sunset, triple seat.

2.10 Data Analytics on Offenses Info

Huge clusters of data provide extensive insights. Offenses having various attributes can be easily mined for generating:-

1) Habitual driving patterns of drivers.
2) Number of offenses and their severity.
3) No. of road mishaps, accretion/decrease in problems and exactly where, what, how, whom?

2.11 Advantages

They are as follows:-

1. The official has all the devices required. No requirement of paper work at all.

2. Vehicle thefts can be prevented by a much reduced rate than the current system.

3. Data analytics on the Offenses Info will help in forming patterns, taking stringent actions and using it as a *"Modus Operandi"*.

III. PROPOSED SYSTEM IN A NUTSHELL

This application provides the official to make new entries of users to the database with the offenses and the number of times they are caught breaking the traffic rules. This basically helps to keep a track on the history of traffic crimes committed by any individuals, which serves the purpose of R.T.O officials.

Fig.7 Proposed System Working

The important and most foremost is that there should be relatively no or minimal delay involved. More and more officials should be involved to nab the miscreants at various strategic locations in the various corners of the city. Also, the system is slightly costlier but to counter the outnumbering vehicle thefts would be incomparable indeed. It is essential that the number of vehicle thefts need to be curbed and this system offers a more approachable and crisp solution.

IV. DESIGN ASPECTS

4.1 Class Diagram

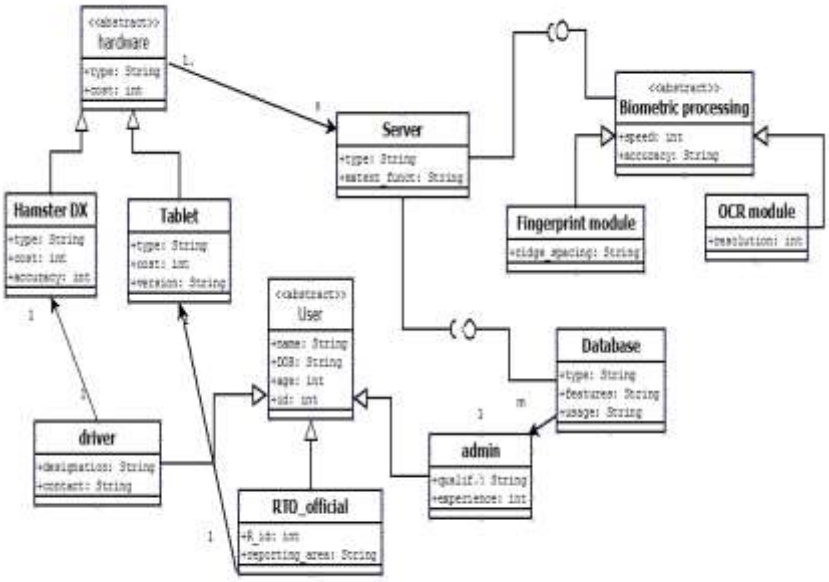

Fig.8 Class Diagram of the system

The class diagram consists of the different classes which are namely the Server, the databases, scanner, the OCR modules and different users of the system. The class diagram denotes the components, connectors and configuration of the system with the client-server Architectural style.

4.2 Flowchart

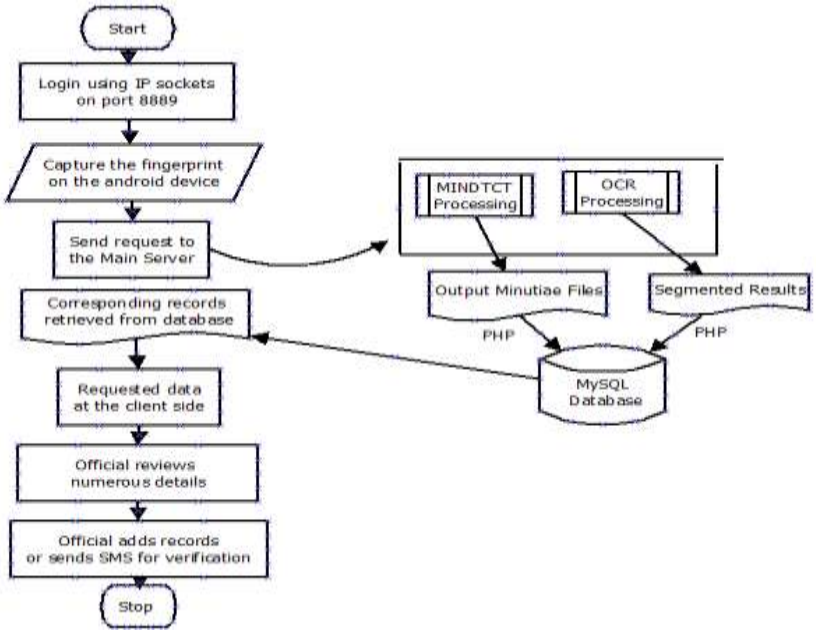

Fig.9 Flowchart of the System

The flowchart of the system consists of the process of the biometric identification system (BIS) involving the peripheral device, the fingerprint recognition module and OCR modules.

4.3 Use Case Diagram

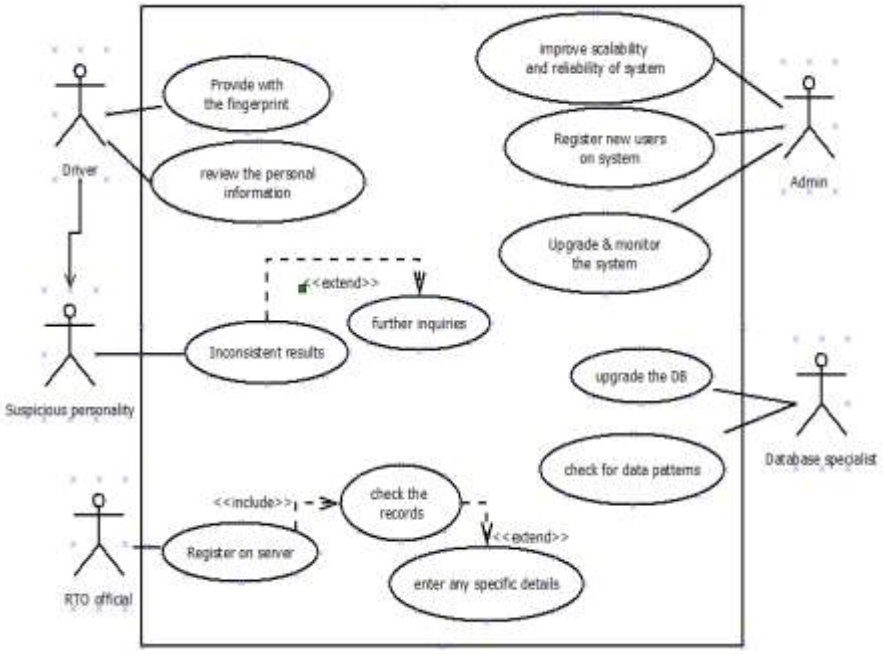

Fig.10 Use Case Diagram

Use case diagram consists of User or driver, both malicious and benign, official, DB specialist and Admin. These are the entities that are interacting with the system. The various use cases implemented are by the individual actors in the system.

V. IMPLEMENTATION ASPECTS

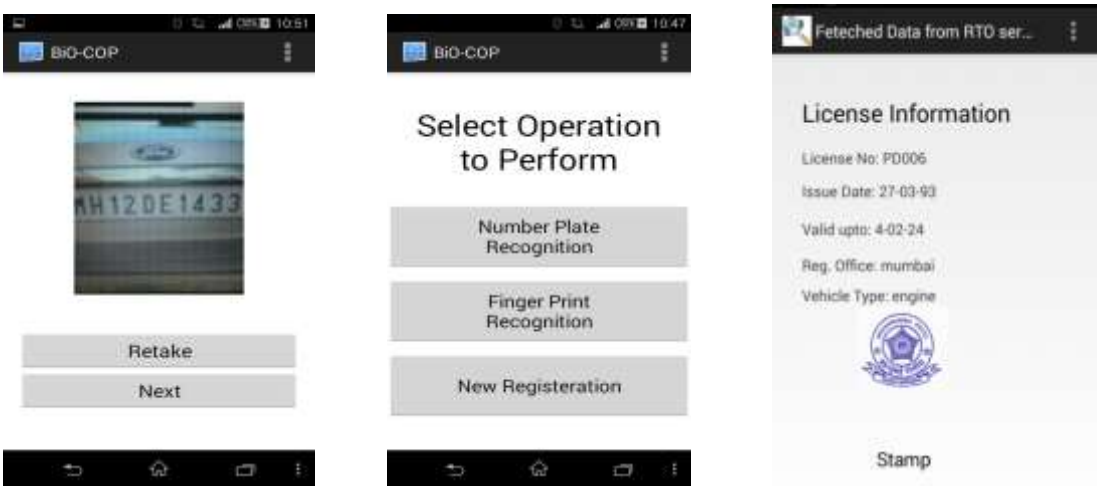

Fig.11 A) Activate Camera For Number Plate Capture. B) Select any of The 3 Options Mentioned. C) Display of Licence Info From The Server

Number-plate Recognition consists of activating the camera and performing the OCR. Fingerprint Recognition consists of obtaining the biometric via a peripheral device and using Bozorth3 algorithm on it. Lastly, a new Registration is added to the main database server for any new inclusions to the already available information. The type of offence is also specified in the new entry as shown in Fig.11.

As shown in Fig.12; it shows some snapshots of the app which would be used by the traffic policeman.

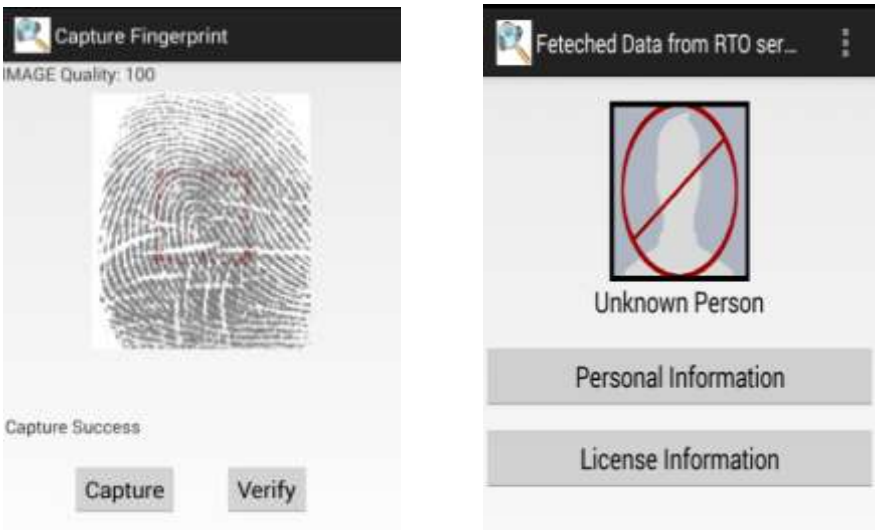

Fig.12 A) Fingerprint Capture; Here Square Box Focuses on Capturing Core Points. B) Not Registered

VI. CONCLUSION

The era of fingerprints continues to be a booming field with its ever growing applications in several domains especially banking and commercial uses. But licence management is still devoid of the advent of mobile biometrics based android app. Unlike the existing system of carrying documents, which can get misplaced, the genuineness of the documents can be verified at any instant, thus this proposed system eliminates the demerits and provides an instantaneous and lucid solution.. This is also supported by Optical Character Recognition

which helps the application to extract details about any vehicle by preventing or reducing any vehicle thefts, offenses, road mishaps and greater misery to what already exists.

REFERENCES

[1] Wayman, James, Anil Jain, Davide Maltoni, and Dario Maio. "An introduction to biometric authentication systems." In Biometric Systems, pp. 1-20. Springer London, 2005.

[2] Jain, Anil K., Lin Hong, Sharath Pankanti, and Ruud Bolle. "An identity-authentication system using fingerprints." Proceedings of the IEEE 85, no. 9 (1997): 1365-1388.

[3] Ashwin, S., S. Loganathan, S. Santosh Kumar, and P. Sivakumar. "Prototype of a fingerprint based licensing system for driving." In Information Communication and Embedded Systems (ICICES), 2013 International Conference on, pp. 974-987. IEEE, 2013.

[4] Al-Hamdani, Osamah, Ali Chekima, Jamal Dargham, Sh-Hussain Salleh, Fuad Noman, Hadri Hussain, A. K. Ariff, and Alias Mohd Noor. "Multimodal Biometrics Based on Identification and Verification System." Journal of Biometrics & Biostatistics 4, no. 2 (2013).

[5] Mansfield, Tony, and Marek Rejman-Greene. "Feasibility study on the use of biometrics in an entitlement scheme." National Phys. Lab., Teddington, UK (2003).

[6] Simao,P. Fonseca, J. Santos and DETI, Univ. de Aveiro, Aveiro."Finger Print Based Driving License Management System."In Consumer Electronics, 2008. ISCE 2008.2008 IEEE International Symposium on,4-16 April 2008,IEEE 2008.

[7] Safronov, Kirill, Ing Igor Tchouchenkov, and Ing Heinz Wörn. "Optical Character Recognition Using Optimisation Algorithms." In Proceedings of the Ninth International Workshop on Computer Science and Information Technologies, Russia, pp. 1-5. 2007.

[8] Alonso-Fernandez, Fernando, Josef Bigun, Julian Fierrez, Hartwig Fronthaler, Klaus Kollreider, and Javier Ortega-Garcia. "Fingerprint recognition." In Guide to biometric reference systems and performance evaluation, pp. 51-88. Springer London, 2009.

[9] Eikvil, Line. "Optical Character Recognition." citeseer. ist. psu. edu/142042. html (1993).

[10] "USB Fingerprint Scanner-Fingkey Hamster DX",BioEnable Technologies Pvt. Ltd ,accessed September 28,2014,http://www.bioenabletech.com/usb-fingerprint-scanner.

[11] Rubella, J. Angeline, M. Suganya, K. Senathipathi, B. Santhosh Kumar, K. R. Gowdham, and M. Ranjithkumar. "Fingerprint based license checking for auto-mobiles." In Advanced Computing (ICoAC), 2012 Fourth International Conference on, pp. 1-8. IEEE, 2012.

[12] Biometric Residence Permits General Information for Applicants,Employers and Sponspors, Information Leaflet,UK:Home Office ,July 2013.

[13] Warren, Adam, and Elizabeth Mavroudi. "Managing surveillance? The impact of biometric residence permits on UK migrants." Journal of Ethnic and Migration Studies 37, no. 9 (2011): 1495-1511.

[14] Watson, Craig I., Michael D. Garris, Elham Tabassi, Charles L. Wilson, R. Michael Mccabe, Stanley Janet, and Kenneth Ko. "User's guide to NIST biometric image software (NBIS)." (2007).

[15] Jain, Anil K., Arun Ross, and Salil Prabhakar. "An introduction to biometric recognition." Circuits and Systems for Video Technology, IEEE Transactions on 14, no. 1 (2004): 4-20.

[16] Phillips, P. Jonathon, Alvin Martin, Charles L. Wilson, and Mark Przybocki. "An introduction evaluating biometric systems." Computer 33, no. 2 (2000): 56-63.

[17] "Fingerprint recognition." Wikipedia, The Free Encyclopedia. Wikimedia Foundation, Inc. 10 September 2014. Web. 10 Aug. 2004.

[18] Yang,Li.(2015). *NFIS2 Software* [PowerPoint slides]. Retrieved fromhttp://web2.utc.edu/~Li-Yang/cpsc4600/2-FingerPrint/NBIS.ppt.

[19] "Cygwin FAQ." Cygwin FAQ. N.p., n.d. Web. 23 Mar. 2015.[online].Retrievedfrom http://cygwin.com/faq/faq.html#faq.what.what.

[20] "Biometrics." Wikipedia, The Free Encyclopedia. Wikimedia Foundation, Inc. 10 September 2014. Web. 10 Aug. 2004.

[21] biometric reference system for fingerprint NIST Fingerprint Image Software 2. (2015). 1st ed. [ebook] BioSecure, pp.1-10.Available at:http://svnext.it-sudparis.eu/svnview2- eph/ref_syst/Fingerprint _NIST/doc/how To.pdf. [Accessed 7 Apr. 2015].