International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 1, Issue 2, October 2014

A Study of Biometric Approach for Vehicle Security System Using Fingerprint Recognition

N. Kiruthiga[1] and L. Latha[2]

M.E, Department of CSE, Kumaraguru College of Technology, Coimbatore, India [1]

Associate Professor, Department of CSE, Kumaraguru College of Technology, Coimbatore, India [2]

Abstract*:* The use of vehicle is a must for everyone. In the same way, safeguarding the vehicle against theft is also very essential. Impediment of vehicle theft can be done remotely by an authorized person. Embedded computing technology is an emergent field used in all the areas. A competent automotive security system is implemented using embedded system along with Global System for Mobile (GSM) and Fingerprint Recognition. This paper gives a literature survey on the vehicle security system using person identification techniques. The survey mainly emphasizes on major approaches for automatic person identification, namely fingerprint recognition and various existing vehicle security system. The security system can be implemented using Microcontroller.

Keywords: Microcontroller, Attention (AT) Command, Global System for Mobile (GSM) and Anti-theft Mechanisms.

I. INTRODUCTION

Automated person identification or recognition has become popular in recent years because of its applications like protected access to computer systems, buildings, cellular phones and in terms of security like video surveillance. Person identification is the process of providing identity to an individual. Person identification techniques are broadly classified into three, knowledge based, token based and biometric based. A knowledge based approach depends on something that an individual knows to make a personal identification like password or personal identification number (PIN). Token – based approaches are based on something an individual have like passport, driving license, ID card, credit card or keys. But these approaches have lot of demerits: tokens may be stolen, lost, elapsed or mislaid. But the biometric systems use physiological or behavioural characteristics of an individual for identification and it cannot be stolen or lost.

Fingerprint based identification is one of the most important biometric technologies which have drawn an extensive amount of attention recently. Fingerprints are believed to be unique across individuals. Fingerprint biometrics provides robust, reliable and foolproof personal identification. There are two types of fingerprint systems: fingerprint verification and identification. Fingerprint verification is the process of accepting and rejecting the identity claim of a person using his/her fingerprint (one-to-one matching). Fingerprint identification, on the other hand, is the process of determining which registered individual provides a given fingerprint (many-to-one matching) [1].

Fingerprint biometrics is one of the efficient, secure, cost effective, ease to use technologies for user authentication. Because of the intellectual property protection and commercial profits, it can also be used in the field of automobiles for providing security and theft protection.

The main component (BRAIN) of the security system is PIC (Peripheral Interface Controller) microcontroller. It is responsible for all monitoring and generating the inputs and outputs respectively. The output of the system will be displayed on LCD of SMS arrival status and configuration etc. Proper LCD display is obtained through programming and LCD interface design. Totally three trials will be given to the user and if the scan matches access will be given. Else if intruder is using and three trials are failed then alert message will be sent to the owner's vehicle. On receive SMS from owner; the alarming system will be activated. In case of network error on the owner

position, the second alert message may be sent to nearby police station.

II. Related Work On Fingerprint Biometric In Vehicle Security

The recent developments in biometrics recognition lead to improvements in reliability and accuracy. The related works for Fingerprint Recognition (FR) for vehicle security system are summarized in this section.

A. Existing Security Systems for Vehicles

Different anti-theft systems have been developed over the past few years. Intelligent Computerized anti-theft system [ICAT] which uses the concept of Radio frequency Identification (RFID) is implemented in many vehicles. The limitation here is that keyless RFID cards can be easily stolen. In addition, key may malfunction when it is in contact with metallic object [19].

An Info-Security Circuit Board which communicates with Engine Control Unit (ECU) and sensors inside the vehicle Bus, Flex Ray and most of the bus communicates with other vehicles, road-side infrastructure and cellular phones with wireless interfaces. The shortcoming with this system is that the data timeliness and network delays to realize reliable secure car communications [20].

Some systems use Auto cop mechanism which is a video surveillance solution that can be fitted into the vehicle. The camera will continuously monitor the actions within the system. The main drawback of this system is the camera will not detect accurately when there are changes in the lighting conditions in and around the system [21].Other systems include in-vehicle anti-theft component that will not enable the functions of the appliances if it find itself is illegally moved to another car. The negative aspect of this system is that it requires a secure processor and smart card chips to store in the Group Identification Number [22]. The advanced system uses the Global Positioning System (GPS) to track the position of the targeted vehicle and its current location. GPS uses global navigation satellite system. The location information provided by GPS system can be visualized using Google earth. The main complication of using GPS is that the signal can become degraded and receiver system will not provide location if view of the sky is severely limited. It is also influenced by other factors like rainfall, fog and snowfall [23].

Since other biometrics has their own demerits, the fingerprint recognition technique is unique and it provides higher security and accuracy. In addition, the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are also minimized.

III. Fingerprint Recognition

The main modules of fingerprint verification system are:

a. *Fingerprint sensing,* in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a digital representation.
b. *Pre-processing,* in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction.
c. *Feature extraction,* in which the fingerprint is further processed to generate discriminative properties called feature vectors.

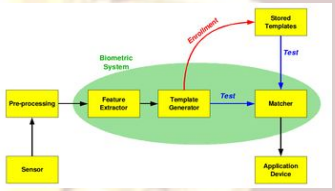


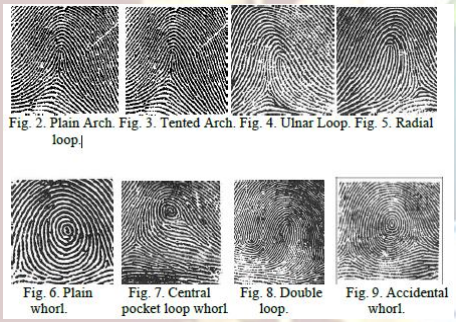
Fig. 1 Representation of Biometric System [2]

d. *Fingerprint matching,* in which feature vector of the input fingerprint is compared against one or more templates. These templates are stored in the database.

The fingerprint matching techniques are minutiae based matching and pattern matching. Pattern matching compares two images for checking similarity. The minutiae matching relies on minutiae points i.e. location and direction of each point [24]. The habitual FP pattern types are represented below:

1. *Plain Arch and Tented Arch:* Plain Arch is a pattern that has ridges at one side, make a rise at the centre, and flow or tend to flow towards the opposite side. Tented Arch has resemblance to plain arch but, ridges create an angle or a steep thrust.
2. *Radial Loops and Ulnar Loops:* Ulnar loop pattern

3. loops shown flow in the direction of little finger, while in Radial loop pattern loops flow in the direction of the thumbs.
4. *Plain Whorl:* Consists of pattern with two deltas and minimum one ridge will make a complete circuit of spiral, oval or any form of circle.
5. *Central Pocket loop Whorl:* It has a pattern with minimum one recurving ridge or an obstruction at right angles to the line of flow.
6. *Double Loop Whorl:* It is distinguished with two separate loop formations. It is composed of two separate and distinct sets of shoulders and two deltas.
7. *Accidental Whorl:* It is the only pattern which is connected with minimum two deltas. It unites two or more distinctive type of patterns excluding the plain arch.



Most of the fingerprint technologies are based on Minutiae. Minutiae-based techniques represent the fingerprint by its local features like terminations and bifurcations. The basic methods of minutiae extraction is divided into following steps:

Step 1: Input

In this step, fingerprints of persons are taken as input and processed.

Step 2: Binarization

This transforms the 8-bit Gray fingerprint image to a 1-bit image with 0- value for ridges and 1-value for furrows.

Step 3: Thinning

Ridge thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide.

Fig-10 (a) Original image, (b) normalized image, (c) Binarized image, (d) Thinned image

Step 4: Minutiae Connect:

This operation takes thinned image as input and produces refined skeleton image by converting small straight lines to curve to maximum possible extent.

Step 5: Minutiae Margin:

This increases the margin of endpoints by one pixel of curves of length at least three pixels.

Step 6: Minutiae point Extraction:

For extracting minutiae point, the number of one-value of every 3x3 window is computed:

- If the centre point is 1 and has only 1 one valued neighbour, then the central pixel is a termination.
- If the centre point is 1 and has 3 one-value neighbours, then the central pixel is a bifurcation.
- If the centre point is 1 and has 2 one-value neighbours, then the central pixel is a usual pixel.

Step 7: False Minutiae Removal

Procedure for removing false minutiae is given below. On considering average inter-ridge width D:

If the distance between one bifurcation and one termination is less than D and the two minutiae are in the same ridge both of them should be removed. If the distance between two bifurcations is less than D and they are in the same ridge, then the two bifurcations should be removed.

- If two terminations are located in a short ridge with length less than D, then two terminations should be removed.
- If a branch point has at least two neighbouring branch points, which are each no further away than maximum distance threshold value and these branch points are closely connected on common line segment then the branch points should be removed.

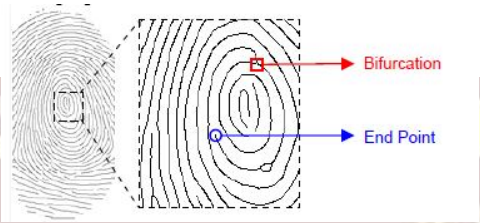


Fig. 11 Detected minutiae [27]

The performance comparison of Biometri technologies based on FAR (False Acceptance Rate), FRR (False Rejection Rate), EER (Equal Error Rate) is given below:

Equal Error Rate –Rate at which both acceptance and rejection errors are equal. Lower the EER, system is more accurate.

False Acceptance Rate – Rate at which system incorrectly matches the input patterns to non-matching template in the database.

False Rejection Rate – Rate at which system fails to detect match between input pattern and matching template in the database.

TABLE I
TABLE I- PERFORMANCE COMPARISON OF VARIOUS BIOMETRICS [26]

BIOMETRICS	EER	FAR	FRR	COMMENTS
Face	NA	1%	10%	Varied light, indoor/outdoor
Fingerprint	2%	2%	2%	Cut on fingers
Hand Geometry	3%	5%	2%	Rings & improper placement
Iris	0.01%	0.94%	0.99%	Indoor environment
Keystrokes	1.8%	7%	0.1%	6 months period
Voice	6%	2%	10%	multilingual

The related work for Fingerprint Recognition (FR) analysed with different parameters such as matching techniques, recognition methods, retrieval concepts, security and the like are summarized below:

A correlation based Fingerprint Recognition system can be used for "feature extraction". The scheme uses Gabor filters for Fingerprint feature extraction. The test results of low FAR, FRR and 97% accuracy are reported [2] A concept for FR using digital camera is introduced. The Gabor features obtained by the Gabor filters are compressed using PCA and then matching is performed with the help of cosine angle. It reports improved result in terms of segmentation, enhancement and core point detection [16].

A secured approach for FR based on set of assembled geometric moment and Zernike moment is proposed. The results on FVC2002 database show EER=2.27%, average enrolment time=1.77s and average match time=0.19s [3].

A novel methodology for "partial FP matching" based on pores corresponding to their Local Binary Pattern (LBP) features is developed. The NIST SD30 database result is tested and best match score is obtained [4] The cross matching performance of the auxiliary data AD of the Fuzzy Commitment Scheme (FCS) has been analysed. The result on MCYT database shows that cross matching performance is not as good as system performance [5]. Various strategies related to key binding with QIM in a BE context are examined. The obtained results demonstrate that the QIM method facilitates tuning of the system performance [6].

The Fingerprint Recognition using Euclidean distance method has been proposed. The test results show a precision of 95% for the ST-BIO Card Reader Model: BCR100T V3.0, and 85% for the VeriFinger Sample DB database. The average access time reported is 19.68 seconds per image [7].

A provably secure and blind biometric authentication protocol, which addresses the concerns of user's privacy, template protection and trust issues, has been formulated. Experimental results on four biometric datasets (face, iris, hand geometry, and FP) showed that the authentication in the encrypted domain does not affect the accuracy [8].

A method for increasing matching speed by compressing spectral minutiae feature using Column PCA (Principal Component Analysis) and Line DFT (Line Discrete Fourier Transform) reduction techniques is proposed. The reduction rate of 94% and a speed of 125000 comparisons per second is reported and the experimental results on MCYT database show EER=0.29%, FAR=99.8% and on FVC2002-DB2 database show EER=3.72%, FAR=95.6% [9].

A method to access the effect of water-induced finger that degrades the performance of minutiae-based FR system is devised. The test results show EER on dry finger 2.13% and wrinkled finger 3.15%. The True positive rate (TPR) 96.7% for dry finger and 72.4% for wrinkled finger is reported [11].

A practical secure data retrieval and authentication techniques for complex distributed systems has been

illustrated. The test report ERR=8%, FAR=13.7% and FRR=3.8% [12].

A visual threshold cryptographic method to keep compressed FP template information securely at the server to avoid hacking has been identified. Lossy compression technique DCT is used for compressing. The results prove FAR and FRR of 0.2% and better efficiency reduces falsification and maintenance cost [13].

The problem of fast FP retrieval in a large database using clustering-based descriptors has been evaluated. The experimental results on NIST database using SVN classifiers and orientation image report the accuracy of 86.68% and fastest matching time 0.056s [14].

The performance of reusable biometric security systems, in which the same biometric information is reused in multiple locations, is analysed [15]. Very powerful algorithms for both full and partial fingerprints are introduced. The test result using Spaced Frequency Transformation Algorithm (SFTA) based on the Fast Fourier Transform of the images and Line Scan Algorithm (LSA). The result reports 95% accuracy for partial Fingerprints and 97% accuracy for full Fingerprints [17, 25].

IV. WORKING OF THE SECURITY SYSTEM

The security system mechanism contains two modes: first, if the system is active and an unauthorized person tries to turn on the vehicle, then alert message will be sent to the registered user in system and vehicle will be in OFF condition. In second mode, authorized person can will be authenticated and given access.

The main component (BRAIN) of this system is PIC (Peripheral Interface Controller) microcontroller. It is responsible for all monitoring and generating the inputs and outputs respectively. The output of the system will be displayed on LCD (Liquid Crystal Display).

Proper LCD display is obtained through programming and LCD interface design. Totally three trials will be given to the user and if the scan matches access will be given. Else if intruder is using and three trials are failed then alert message will be sent to the owner's vehicle. On receive SMS from owner; the alarming system will be activated. In case of network error on the owner position, the second alert message may be sent to nearby police station.

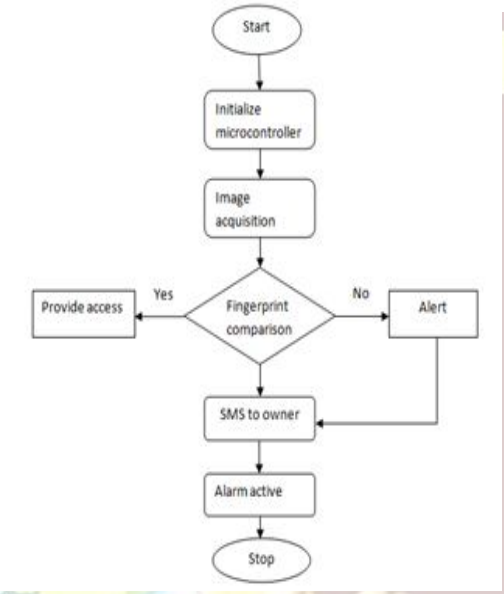


Fig. 12 Flow chart for the security system

Proper LCD display is obtained through programming and LCD interface design. Totally three trials will be given to the user and if the scan matches access will be given. Else if intruder is using and three trials are failed then alert message will be sent to the owner's vehicle. On receive SMS from owner; the alarming system will be activated. In case of network error on the owner position, the second alert message may be sent to nearby police station. The serial communication is provided by RS232 cable. It interfaces the programming to the prototype model. The interfacing between microcontroller and GSM is through UART (Universal Asynchronous Receiver Transmitter) communication which is serial communication protocol [5].

V. CONCLUSION

Security is becoming essential in all kind of application. This project is aimed at improving the security level. As the fingerprint is a promising biometric pattern for personal identification in terms of both security and ease of use. This is a unique method of designing and assembling a low-cost, compact theft control system for an automobile. The work presented demonstrates the initial phase of an embedded car that will be visible in near future. Customized

vehicles will not only provide a more interesting drive but also safer one.

This paper presented the performance analysis for fingerprint biometric. It presents apparent advantages over password and token-based security. The survey represented the issues associated to uni-modal biometric systems. It can be concluded that automatic Fingerprint recognition is the biometric technology that can be used for security in terms of usability, size, privacy and operational temperature range. The proposed security system can be used to reduce the increased vehicle theft and allows the owner to identify the intruder thereby having the vehicle under his/her control.

It is applicable to car, truck, armoured vehicle, yacht, boat or heavy equipment vehicle. The system is also reliable to be used in other authorization applications involving robotics, border management, banking security involving ATMs etc.

REFERENCES

[1] Z. M. Win and M. M. Sein, "Fingerprint recognition system for low quality images", presented at the *SICE Annual Conference*, Waseda University, Tokyo, Japan, Sep. 13-18, 2011.

[2] http://en.wikipedia.org/wiki/Biometrics.

[3] Megha Kulshrestha and V.K. Banga, "Finger Print Recognition: Survey of Minutiae and Gabor Filtering Approach", *Int. Journal of Computer Applications(1995-8887)*, Volume 50-No.4, July 2012.

[4] J. C. Yang, N. X. Xiong, A. V. Vasilakos and Zh. J. Fang, "A fingerprint recognition scheme based on assembling invariant moments for cloud computing communications", *IEEE Systems Journal*, vol. 5, no. 4, Dec. 2011.

[5] S. Malathi and C. Meena, "An efficient method for partial fingerprint recognition based on Local Binary Pattern", in *Proc.Communication Control and Computing Technologies*, pp. 569-572, IEEE, 2010.

[6] E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, and R. N. J. Veldhuis, "Preventing the decodability attack based cross-matching in a fuzzy commitment scheme", *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, IEEE, March 2011.

[7] F. M. Bui, K. Martin, H. P. Lu, K. N. Plataniotis, and D. Hatzinakos, "Fuzzy key binding strategies based on quantization index modulation(QIM) for biometric encryption (BE) applications", *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, IEEE, March 2010.

[8] C. Pornpanomchai and A. Phaisitkulwiwat, "Fingerprint recognition by euclidean distance", presented at *Second International Conference on Computer and Network Technology, IEEE*, 2010.

[9] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar, "Blind Authentication: A secure crypto-biometric verification Protocol", IEEE *Transactions on Information Forensics and Security*, vol. 5, no. 2, June 2010.

[10] H. Y. Xu, R. N. J. Veldhuis, T. A. M. Kevenaar, and T. A. H. M. Akkermans, "A fast minutiae-based fingerprint recognition system", *IEEE Systems Journal*, vol. 3, no. 4, Dec. 2009.

[11] C. I. Fan and Y. H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics", *IEEE Transactions on Information Forensics and Security*, IEEE, vol. 4, no. 4, December 2009.

[12] H. Fakourfar and S. Belongie, "Fingerprint recognition system performance in the maritime environment", in *Proc. Applications of Computer Vision*, IEEE, 2009, pp1-5.

[13] B. K. Sy, "Secure computation for biometric data security : application to speaker verification", *IEEE Systems Journal*, IEEE, vol. 3, no. 4, December 2009.

[14] R. Mukesh and V. J. Subashini, " Fingerprint based authentication system using threshold visual cryptographic technique", in *Proc. IEEE-International Conference on Advances in Engineering, Science and Management*, Mar 30-31, 2012, pp. 16-19.

[15] R. Y. Zheng, C. Zhang, S. H. He, and P. W. Hao, "A novel composite framework for large-scale fingerprint database indexing and fast retrieval", in *Proc. Hand-Based Biometrics*, IEEE, 2011, pp. 1-6.

[16] L. F. Lai, S. W. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems, part II: multiple use case", *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, March 2011.

[17] B. Y. Hiew, A. B. J. Teoh, and Y. H. Pang, "Digital camera based fingerprint recognition", in *Proc. the 2007 IEEE International Conference on Telecommunications and Malaysia Conference on Communications*, Penang, May 14-17, 2007.

[18] S. Mil'shtein, A. Pillai, A. Shendye, C. Liessner, and M. Baier, "Finger print recognition algorithms for partial and full fingerprints", in *Proc. Technologies for Homeland Security*, IEEE, 2008, pp. 449-452.

[19] Upendran Rajendran and Albert Joe Francis, "Anti Theft Control System Design Using Embedded System", *Proc. IEEE*, vol. 85, page no. 239- 242, 2011.

[20] Sukeerti Singh and Ayushi Mhalan, "Vehicle Theft Alert System using GSM", *Int. Journal of Engineering Science and Technology (IJEST)*, May 2013.

[21] Vikram Kulkarni and G. Narsimhulu, " A Low cost Extended Embedded Smart Car Security System on Face Detection and Continuous Video Monitoring System", *Int. Journal of Engineering Science and Advanced Technology (IJESAT)*, May 2012.

[22] M.Sunitha, V.Vinay Kumar and G. Raghu, "Embedded Car Security System", *Int. Journal of Engineering Development and Research (IJEDR)*, 2012.

[23] Mohammad A. Al-Khedher and Sharaf A. Al-Kheder,"Intelligent Anti-Theft and Tracking System for Automobiles", *Int. Journal of Machine Learning and Computing*, February 2012.

[24] Megha Kulshrestha and V. K. Banga, "Finger Print Recognition: Survey of Minutiae and Gabor Filtering Approach ",*Int. Journal of Computer Applications (0975 – 8887) Volume 50 – No.4, July 201*.

[25] Kaisheng Zhang, "Study on the Embedded Fingerprint Image Recognition System", *Int. Conference of Information Science and Management Engineering, 2010*.

[26] Sruthi Sebastin," Literature Survey on Automated Person Identification Techniques", *Int. Journal of Computer Science and Mobile Computing*, Vol. 2, Issue. 5, May 2013, pg.232 – 237.

[27] Susheel Jain and Anurag Jain, "Literature Survey on Fingerprint Recogniyion Using Level 3 Feature Extraction Method", *Int. Journal of Engineering and Computer Science ISSN:2319-7242*, Volume 3, January 2014.

BIOGRAPHY

Ms. N. Kiruthiga, have completed her B.E (Computer Science & Engineering) in the year 2013 from, Anna University, Chennai. Presently studying Master of Engineering in Computer Science & Engineering at Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India. Her research interests: Biometrics and Embedded Systems.

Dr.L.Latha, presently working as Associate Professor at Kumaraguru College of Technology in the Department of Computer Science & Engineering, Coimbatore, T.N., India. She has 18 years of teaching experience and her research interests include Image Processing, Biometrics and Information Security.