Real Time Smart Car Security System by Using Biometrics

S. P. Pingat, Shubham Rakhecha, Rishabh Agrawal, Sarika Mhetre, Pranay Raushan

Abstract- In this proposed paper, two tier security for car is achieved using Biometrics such as FDS (Face Detection System) and Finger Print Detection System. FDS is used to detect the face of the person driving the car and compare it with the training set. For example, during night when the owner of car is sleeping and someone tries to rob the car then initially the finger print of that person will be detected and matched with predefined image through handle of the car where the Finger print scanner can be placed. Also in case if that person surpass the Finger print security then FDS image obtained by one tiny camera which can be hidden easily somewhere in the car. Image obtained through the camera is then compared with stored (training set) image using FDS. If the image does not get match, then the information is sent to the owner through MMS. The image of the thief can be obtained by owner in his mobile through MMS as well as he can get the location of the vehicle through GPS. The owner can get the location of vehicle through SMS. So by using this system, owner can get the image of thief as well as the Car's Location.

Keywords- FDS (Face Detection System), MMS (Multi Media System), PCA (Principle Component Analysis), GPS (Global positioning System), GSM (Global System for Mobile Communication), Finger Print Scanner.

I. INTRODUCTION

This paper aims at providing high level security which consists of a Face Detection System (FDS), Finger Print Scanner, GPS (Global Positioning System) module, a MMS (Multi Media System) module and a control platform. The Face Detection System is based on PCA algorithm and can detect face of the person driving the car. The other module provides necessary information to owner and help to know the location of the car, even when the car is lost.

This system is built on one embedded platform in which one SoC named "SEP4020" (works at 100MHz) controls all the processes. Experimentally it is evaluated.

This paper will help to achieve high security and reduce theft and cheaper and 'smarter' than older ones.

Manuscript published on 30 March 2013.
***Correspondence Author(s)**

Prof. S. P. Pingat, Computer Department, Smt. Kashibai Navale College Of Engineering, PuneIndia.
Shubham Rakhecha Computer Department, Smt. Kashibai Navale College Of Engineering , Pune India.
Rishabh Agrawal, Computer Department, Smt. Kashibai Navale College Of Engineering , Pune India.
Sarika Mhetre, Computer Department, Smt. Kashibai Navale College Of Engineering , Pune India.
Pranay Raushan, Computer Department, Smt. Kashibai Navale College Of Engineering , Pune India.

II. INSPIRATION

In current system, the car alarm is used where if the intruder enters the car then alarm starts sound but the car safety is not assured since the range of the sound is limited to parking area. Thus the car once theft can't be assured to recovered back. Presently the Anti-Theft security system is immobilized i.e. monitoring mobile is difficult. Also the statistics of car theft in India shows that after every 26th second a car is stolen which tally total around 12 lakh cars theft per year, out of which only 13 percent cars are recovered. So considering current scenario there is need of Robust Anti-Theft security system. In this paper we are proposing an enhanced version of wireless control anti-theft system using Biometrics.

III. PROBLEM DESCRIPTION

In this proposed system, we introduced a low-cost extendable framework for embedded smart car security system, which consists of a Finger Print Scanner, Face Detection System (FDS), a GPS (Global Positioning System) module, a GSM (Global System for Mobile Communications) module and a control platform. In this system whenever an intruder enters the car, an SMS is sent to the owner of the car as the alert message and this improves the security of the cars.

IV. SYSTEM OVERVIEW

A. Fingerprint Detection System:

In this paper, we will implement a Fingerprint Detection System. This system tries to find the identity of a given Fingerprint according to their memory (Training Set). In this paper, our training set consists of the fingerprint images of the Owner. Thus, the function of the fingerprint recognizer is to find the most similar fingerprint among the training set. Here, we want to find the identity of a person where an image of fingerprint of that person (test image) is given to the system.

B. Face recognition:

In this paper, we will implement a face recognition system using the Principal Component Analysis (PCA) algorithm. The face recognition systems tries to find the identity of a given face image according to their memory (training set). The memory of FDS consists of Training Set. In this paper, our training set consists of known face images of different persons.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Thus, the function of the face recognizer is to find the most similar average face vector among the training set to the average face vector of a given test image. Here, we want to identify the person entering the car by comparing with the person (test image) given to the system.

C. Face Detection:

In this technique, we enroll the face of the owner in to the database (Training set). There can be multiple authorized persons to drive the vehicle, thus image of all the persons can be stored into the training set. For image recognition and compression the Principal Component Analysis (PCA) is one of the most widely used techniques. The PCA aims at reducing the large dimensionality of the data space (observed variables) to the smaller intrinsic dimensionality of average face (independent variables), which can describe the data economically.

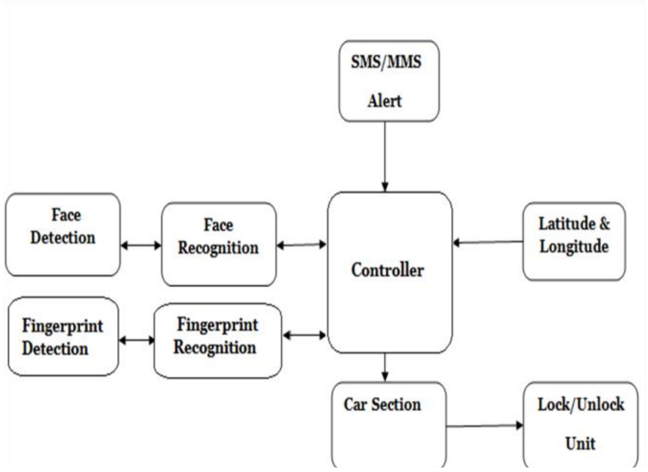

Figure 1.Architecture Diagram

D. MMS Module:

In case if the face of the person does not match with the training set, System will send a bit suggesting entry of unauthorized person in the car and thus it will activate the MMS module present in that system. The role of MMS module is to send the image of that unauthorized person on the owner's Mobile. Owner will response to this MMS through text, suggesting whether to stop the car or continue it.

E. GPS Module:

The role of this Module is to locate the current position of the car and thus send the GPS coordinates through GSM module to the owner. Thus it will guide the owner about the car's location.

V. IMPLEMENTATION

In the Real time proposed system, a Finger Print device will be placed on the door of the car in order to capture and match the finger print of the person entering the car. In case if some unauthorized person bypass the fingerprint security and enters the car, then a hidden web-cam will capture his/her image and compare it with database (Training Set). If the image does not get matched with the database image, then using MMS module it will send the image of that person to the owner. Also the owner will receive the exact location of the car using GPS module. Now the owner can stop the car by sending SMS to the control platform.

In our paper, we are implementing above proposed system on 8051 microcontroller kit which will handle the control of MMS and GPS module. Using web-cam we can capture the image of the person and then compare that image using PCA algorithm in MATLAB. Also Fingerprint Scanner will allow us to provide two level security.

VI. PCA ALGORITHM

A. Overview:

PCA tries to identify the directions of maximum variation in the training data. By using PCA algorithm, a specific face can be recognized by comparing the principal components of the current face to those of the known individuals in a facial database built in advance.

B. Steps of PCA Algorithm:

Step 1: Choose a training set (database) that includes a number of images (M) for each person with some variation in pose and different faces.

Step 2: Convert the training set into the face vector space matrix of M*N2 size where m indicates number of images (column) and N2 indicates size of image (row).

Step 3: Convert the face vector space into normalize face vector.

Step 4: Combine the normalized training set of images to produce M' Eigen faces.

Step 5: Store these Eigen faces for later use.

Step 6: For each member in the face database, compute and store average face vector.

Step7: Choose a threshold value 'e' that defines the maximum allowable distance from any face class. Optionally choose a threshold 'f' that defines the maximum allowable distance from face space.

Step 8: For each new face image to be identified, calculate its average face vector and compare it with the stored average face vectors of the training set.

Step 9: If the comparison satisfies the threshold for at least one member, then classify this face image as "known", otherwise a miss has occurred and classify it as "unknown".

C. Methodology used in PCA Algorithm:

1. Data Acquisition
2. Subtract the mean image data
3. Find the covariance matrix

D. Why PCA:

1. Pattern in data of high dimension
2. Most efficient technique for dimension reduction
3. High data compression
4. Image represent in lower dimension data
5. Reduce complexity of grouping image
6. No data redundancy

VII. FEATURES

1. Enhanced Wireless Control System
2. Availability: wide range of monitoring as based on mobile GSM network.
3. Reliability: Two tier security is highly reliable.
4. Portability: This system can be easily implemented in different cars.

*Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)*

5. Scalability: The system can be easily transformed to three-tier security system.
6. Less cost and compact.

VIII. CONCLUSION

Thus, this paper helps us to enhance and upgrade the security of the car. Also we have implemented Fingerprint and Image-Recognition techniques that can provide the important functions required by advanced Car Security, to avoid vehicle theft and protect from the unauthenticated users**.** Using this system, we can find the image of the thief and exact location of the car. We can also avoid the theft by using this system in our day to day life. This paper will help to achieve high security and reduce theft and cheaper and ‘smarter’ than older ones.

REFERENCES

1. S. Ajaz, M. Asim, M. Ozair, M. Ahmed, M. Siddiqui, Z. Mushtaq, “Autonomous Vehicle Monitoring & Tracking System,” SCONEST 2005, pp. 1 – 4, 2005.
2. Joseph A. O'Sullivan, Robert Pless, “Advances in Security Technologies: Imaging, Anomaly Detection, and Target and Biometric Recognition”, Microwave Symposium IEEE/MTT-S International Volume, Page(s):761 – 764, 2007.
3. Sergey Kosov, Kristina Scherbaum, Kamil Faber, ThorstenThorma¨hlen, and Hans-Peter Seidel, 2009, “Rapid stereo-vision enhanced face detection”. in Proc. IEEE International Conference on Image Processing, pp.1221–1224.
4. Sergey Kosov, Thorsten Thorma¨hlen, Hans-Peter Seidel, 2009,“Accurate Real-Time Disparity Estimation with Variational Methods”, in Proc. International Symposium on Visual Computing, pp.796–807.
5. T.-H. Sun, M. Chen, S. Lo, and F.-C. Tien, 2007, “Face recognition using 2D and disparity eigenface”, Expert Syst.Appl.,vol.33,no.2, pp.265–273.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)