

Government Security using Face Authentication and Card Scanner

Kaushal J. Kashikar¹ Aaditya G. Boradia² Shashank N. Angane³ Sarthak S. Desai⁴

^{1,2,3,4}Thakur Polytechnic, Kandivali (E)

Abstract— Government systems consist of highly sensitive data which should not be altered or compromised or accessed by anyone at any cost. To safeguard the confidentiality of such sensitive data a high end security system is required. One form of authentication cannot be used for such a high end security system. In such cases we must use more than one form of authentication. This system improves the security for secure government data by combining two different forms of security parameters ie via: biometrics + smart cards. The system tends to use face recognition algorithms such as eigen values and eigen vectors to identify user face and then allow him to swipe his smart card in front of a scanner in order to get access. User needs to authenticate himself through both the forms of authentications in order to get access to the system. The user gets access only if he clears both the stages. Thus this system combines two different secure forms of authentication to make a super secure authorization system for government system access.

Key words: Card Scanner, Face Authentication

I. INTRODUCTION

The project allows user to input his face as an image as its password. As soon as the image is received by the system the system segments the image into an array of images and stores them accordingly. The system receives the segmented image in jumbled order when the user next time logs in. Now if user chooses the parts of image in an order so as to make the original image he sent then user is considered authentic. Else the user is restricted from getting access. The system uses image segmentation based on coordinates. According to the segmented image coordinates system stores the fragmented image in different parts. The image is segmented by the system into a grid and each part is stored accordingly in order. But while logging in the image is shown as broken and in a random order. At this time only the user who provided the image knows what the actual image looks like and he must arrange the parts in horizontal direction from left to right one row at a time according to the order in which parts were arranged in the original image. So the user is allowed access after successful attempt.

II. WHAT IS FACE RECOGNITION?

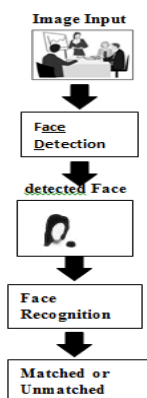


Fig. 1: Face authentication Flowchart

III. EXISTING SYSTEM & PROPOSED SYSTEM

A. Problem with current scenario

1) System Study

System study is a study about existing system. Here we will study in detail about the existing system and its performance.

2) Problem Definition

Face Recognition System is used for biometric security purpose. But for recognized faces properly we required sophisticated face tracing cameras this camera is quit expensive therefore in this project we developed a face recognized system which can recognized the faces based on normal web camera by using Eigen values method.

B. Existing System

- Human guards.
- Police.
- Locks and keys.
- Numeric keypads.
- Magnetic cards / PINs.
- Usernames / passwords.
- Surveillance cameras.

Problems with the Traditional Security Approaches

- Human guards, police are expensive, prone to error and corruption.
- Keys, PINs, passwords can be stolen, lost, or cracked.
- PIN identifies a card and password identifies a username, not user.

Drawbacks of the existing system

- Difficult to maintain the system.
- Can possibly generate inaccurate results.
- User friendliness is very less.

C. Proposed System

Government systems consist of highly sensitive data which should not be altered or compromised or accessed by anyone at any cost. To safeguard the confidentiality of such sensitive data a high end security system is required. One form of authentication cannot be used for such a high end security system. In such cases we must use more than one form of authentication. This system improves the security for secure government data by combining two different forms of security parameters ie via: biometrics + smart cards. The system tends to use face recognition algorithms such as eigen values and eigen vectors to identify user face and then allow him to swipe his smart card in front of a scanner in order to get access. User needs to authenticate himself through both the forms of authentications in order to get access to the system. The user gets access only if he clears both the stages. Thus this system combine two different secure forms of authentication to make a super secure authorization system for government system access.

IV. PROJECT DESIGN

A. E-R Diagram

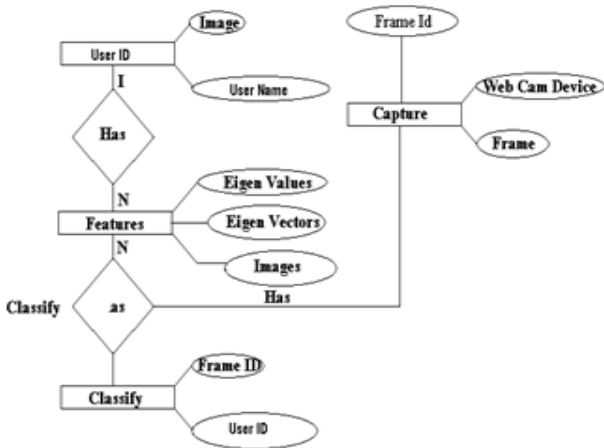


Fig. 2: E-R Diagram

B. System Design

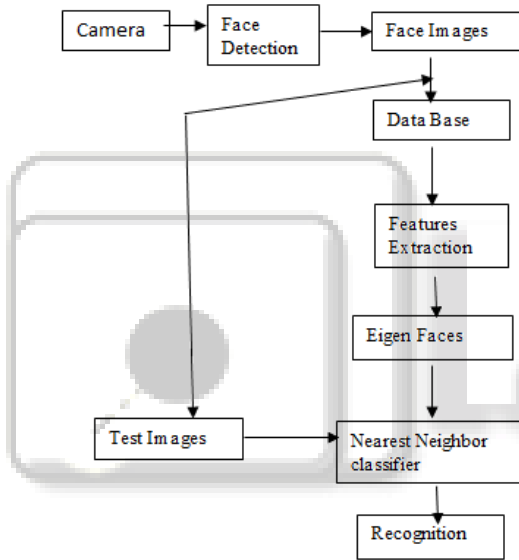


Fig. 3: System Design

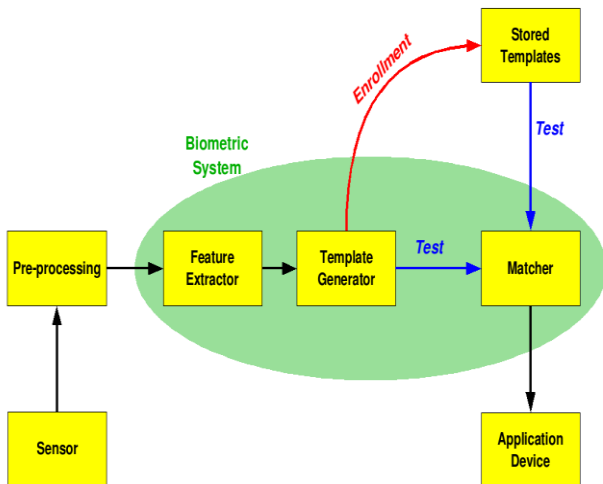


Fig. 4: Biometric Block Diagram

C. Use Case Diagram

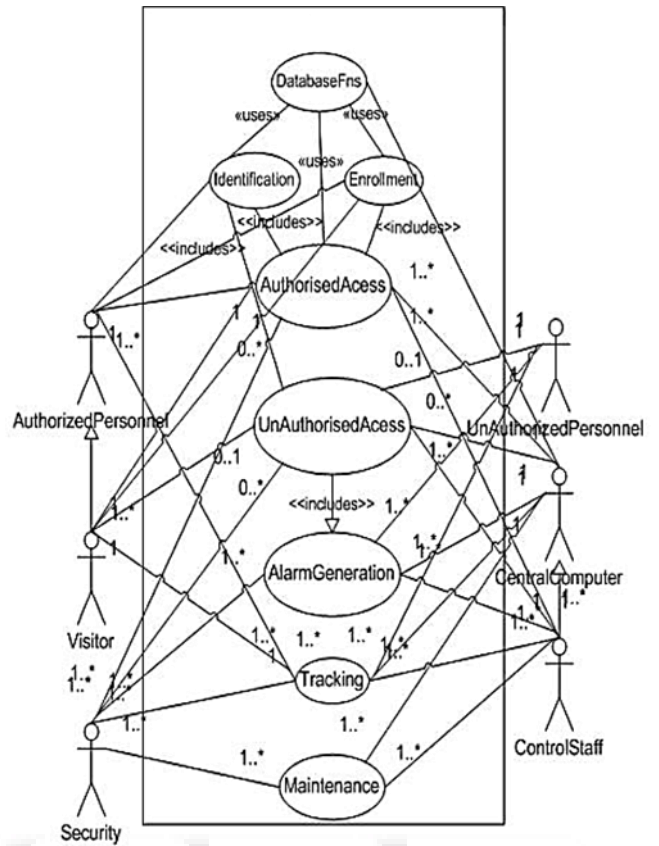


Fig. 5: Use case diagram

D. Sequence Diagram

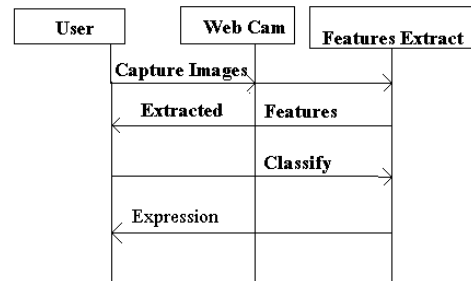


Fig. 6: Sequence Diagram

V. SYSTEM IS

A. Load Balancing:

Since the system will be available only the admin logs in the amount of load on server will be limited to time period of admin access.

B. Easy Accessibility:

Records can be easily accessed and store and other information respectively.

C. User Friendly:

The system will be giving a very user friendly approach for all user.

D. Efficient and reliable:

Maintaining the all secured and database on the server which will be accessible according the user requirement without any maintenance cost will be a very efficient as

compared to storing all the customer data on the spreadsheet or in physically in the record books.

E. Easy maintenance:

Government Security is design as easy way. So maintenance is also easy.

ACKNOWLEDGEMENT

We are pleased to present “Government Security” project and take this opportunity to express our profound gratitude to all those people who helped us in completion of this project.

We thank our college for providing us with excellent facilities that helped us to complete and present this project. We would also like to thank the staff members and lab assistants for permitting us to use computers in the lab as and when required.

We express our deepest gratitude towards our project guide for her valuable and timely advice during the various phases in our project. We would also like to thank her for providing us with all proper facilities and support as the project co-coordinator. We would like to thank her for support, patience and faith in our capabilities and for giving us flexibility in terms of working and reporting schedules.

We would like to thank all our friends for their smiles and friendship making the college life enjoyable and memorable and family members who always stood beside us and provided the utmost important moral support. Finally we would like to thank everyone who has helped us directly or indirectly in our project.

REFERENCES

- [1] en.wikipedia.org
- [2] Microsoft Developer Network (MSDN): <http://msdn2.microsoft.com/en-us/default.aspx>: This is a valuable online resource, and is a must for any developer using Microsoft tools.
- [3] <http://www.asp.net/>: This is the official Microsoft ASP.NET web site. It has a lot of: tutorials, training videos, and sample projects.
- [4] <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6327355&queryText%3Dface+recognition>
- [5] <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6327355&queryText%3Dface+recognition>
- [6] <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5283150&queryText%3Dgovernment+security>
- [7] <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6386949&queryText%3Dsmart+card>