Adaptive Intelligent Authentication System (AIAS)

[1]Giriraj R. Mulay, [2]Anil S. Kale, [3]Ganesh S. Mate, [4]Ravindra P. Tupe
[1,2,3,4]Department of Computer Engineering, Late G.N Sapkal College of Engineering, Nashik, Maharashtra, India.
[1]giririajmulay@gmail.com, [2]anilkale3447@gmail.com, [3]ganesh.mate05@gmail.com, [4]ravitupe21@gmail.com

Abstract **— We have developed an intelligent authentication system for highly confidential data. Our aim is to provide the user with a most secure authentication according to the condition. Normally authentication is based on the biometric Thumb/Finger Detection or Eris Scan considered as most secure way for authentication, but as in the war like condition there may be chance where authorities may be forced to give authentication for system. In such cases where data might be important and life maters too. Here actually we worked on, we have developed an Intelligent Authentication System which is adaptive in nature and can be efficiently used for data security purpose. We are using same biometric mean for normal authentication but in case of emergency we are using a gesture to intimate a system that it has to change its working nature.**

Keywords— Biometric, Eris Scan, Thumb Detection, Gesture Detection, Harr Cascade, Open CV.

I. INTRODUCTION

We have developed an intelligent authentication system for highly confidential data. Our aim was to provide the user with the most secure authentication according to the condition. Normally authentication is based on the biometric Thumb/Finger Detection or Eris Scan considered as most secure way for authentication, but as in the war like condition there may be chance where authorities may be forced to give authentication for system. In such cases where data might be important and life maters too. Here actually we have worked for, we are developing an Intelligent Authentication System which is adaptive in nature and can be efficiently used for data security purpose. We are using same biometric mean for normal authentication but in case of emergency we are using a gesture to intimate a system that it in to change its working nature.

II. HIstory

It was really a challenging job to detect face. And it was more complex when the input face image is noisy or of very low-resolution, camera may not be faced, and with improperly illumination. There are various problems in feature extraction and consequently the face recognition system. Haar-like features are used in proposed system is a novel idea, which have commonly been used for object detection, with a probabilistic classifier of face recognition. The proposed system is real-time, effective, robust and simple against most of the mentioned problems. Experimented results on public databases shows that the proposed system performs the state-of-the-art face recognition systems [1].

They have used Open CV for making dynamic hand gesture detection process quite fast for real time. The whole System is divided into three stages detection and tracking, feature extraction and training and recognition. Representation is a Motion History Image (MHI) that temporally layers consecutive image silhouettes giving the motion properties of a moving person into a single template form. By using Open CV inbuilt functions develop, its recognition rate is quite fast and also the space requirement is low. So the system can be practically used for real time applications [2].

They concluded that a biometric system provides automatic identification of an individual based on a unique feature or characteristic possessed by the individual. Iris recognition is regarded as the most accurate and reliable biometric identification system available. Most commercial iris recognition systems use patented algorithms developed by Daugman, perfect result has been produced by the algorithm recognition rates Digitized grey scale eye image were used for determining the recognition performance of the system [3].

Several issues were investigated related to fingerprint system security including the use of fake fingerprints for masquerading identity, but very little attention is given on the problem of alteration or obfuscation of finger print. Fingerprint obfuscation is nothing but to deliberate alteration of fingerprint pattern by an individual for the purpose of masking his identity. [4]

In a short span of years the industry is growing high with advanced techniques. In that paper they introduces a technique for human computer interaction using open source like python and open CV. The proposed algorithm consists of segmentation, pre-processing, and feature extraction [5].

By referring various papers and various techniques we came to conclusion that there are number of algorithms for authentication of right person but there may the unusual condition where confidential data may be lost. And hence there should be some system where authentication should be given to **right person at right**

situation.

III. EXISTING SYSTEM

Referring to the papers and technologies used for the authentication we have come to the conclusion that all of the best technology for the authentication is biometric that technology there are five types:

- Facial.
- Eris Scan.
- Pin code.
- Thumb detection.
- Palm Detection.

Out of each of has its own importance's and features but they varies in working conditions respectively with their inputs. For example using Eris scan eye structure are scanned and access can be given, if scanned eye is not matched with the database the access is denied and if matches the authentication can be provided, which shows authentication goes for right person. But, it has various disadvantages like pupils may be spread due to presence of extra light factors, if user is using lenses or spectacles then system may fail.

Considering the parameters of all the techniques we discussed till now we come to conclusion that this techniques are the best for authentication purpose but there is common drawback for all the above stated system that right person may get authentication But it may not be at right situation. That is the unauthorized person may force or harm the authorized person to get access to the system.

Need of System

There are various algorithms techniques available to ensure authorization by an appropriate user. But as per our study there is no mean idea to give the authentication as per the situation. The condition may occur that the authentication can be given by right person but not at proper time. He/she may be forced to give the authentication where his/her life may be in danger.

So there is one issue to be under considered, and that is of the time. Let's assume one scenario that an authority has a right to authenticate the system and can access highly confidential data. The authority may be asked to authenticate the system to access the data where his/her life could be challenged. Here we provide exact solution.

IV. PROPOSED SYSTEM

So there should be some technique to handle this situation, we are providing solution for this problem called Adaptive Intelligent Authentication System (AIAS). As it behaves according to situation it is intelligent. For understanding the situation we use gesture to inform system about unusual condition. We have to make system intelligent enough to give authentication to right person at right time.

Our system will check the right person at same it will also check situation and the react accordingly. If it understand that situation is unusual it will simply generate fake data pretend it as if it is real and send notifications to the remote location, live video stream will be shown at remote location so as to understand seriousness of situation.

V. SYSTEM ARCHITECTURE

For informing the system about the unusual condition, user at the victim system has to give a gesture with the thumb which helps system to understand about the situation and it will behaves accordingly.

Here we provide the solution for system to make it adaptive in nature. If there no such unusual condition, means there is no attack like condition than simply user have to give his thumb to access database normally. As shown the following diagram. But, if there is an unusual condition than simply authority have to give a gesture followed by thumb the outcome will be slightly changed. Fake data will be generated with same look and feel of original data. Notifications will be sent at remote place as well as live video stream will be send to remote location with alarm.

While, the attacker may be busy in accessing the fake data which he assumed to be true, with the help of live video streams and notification at remote location situation may be taken under control.

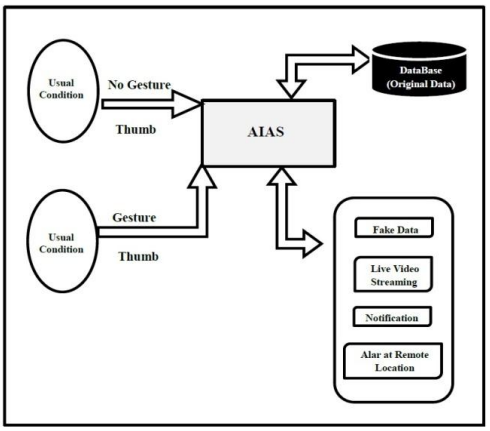

Fig1 System Architecture.

VI. ALGORITHMS

Basically we will discuss the flow of main system based on two conditions:

- Usual Condition (No attack Situation).
- Unusual Condition (Authorized user in danger).

In usual condition authorized user will give thumb for accessing a confidential data. In which the authorized person can easily access the data without giving gesture.

Now below we will discuss algorithm of Thumb detection followed by Gesture Detection.

A Thumb Detection

To detect thumb we are using simple algorithm as we are using Id based device.

Steps for thumb detection:

1. When firstly thumb is scanned a unique Id is generated for each thumb. And is stored in device.
2. Similarly, when the thumb is scanned again then it

is scanned against the template and again new id is created.

3. Whereas the old and current id is matched and authentication is provided.

As the device is id based our work is just to process and check the generated id.

B Gesture Detection

There is need to detect gesture at real time as need of our project. And to detect gesture at real time there is no other better option than using open CV.

Understanding the utilization of the gesture in the project we are using Haar like feature detection Algorithm.

Steps in algorithm

1. Image is passed to the in CV_8U type.
2. The matrix is then scaled using Haar like feature detection.
3. Image is flip.
4. And converted to BGR to Grey. And converted image is passed for processing.
   i. Window of viola-jones object detection is moved on input image.
   ii. Haar like feature is calculated for each sub section it uses integral image (data structure to generate value in rectangular subset of grid for image processing).
   ii. The threshold value is generated (distinguish between objects and non-objects).
   iii. It defines characteristics of certain area of image.
   iv. Lookups and rectangle features are generated I= I(C) + I (A) + I (B) – I (D) Where, A, B, C, D belongs to integral Image I.
   v. Main parts of the faces are calculated using the above steps. All above steps are carried out in haarcascade_FrontalFace_alt.xml of Java CV. Jar library.
5. Now if the last frame and current frame is found different that is mismatch of the pixels then system judge the situation as unusual (as per our project).

VII. RESULT ANALYSIS

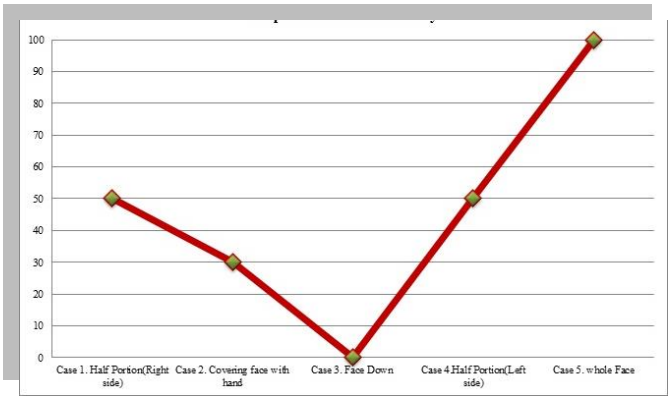

Fig 2. Graph of result analysis.

Case 1: This fig shows one side face which has probablity to cosider it in frame only 50% chance to detect it as face as shown in fig 3. It could be alternative to gesture .So its not considered as face.

Fig.3 Case 1

Case 2: Only half face is shown in Fig. 4 and could be consider as gesture to system. In this eyes are covered by hand to give gesture to system as shown so its not considered as face and is one of the alternative to gesture.

Fig.4 Case 2

Case 3: This fig shows that to recognize the face in image only 0 % face is shown fig. 5 postion is best alternative to a gesture, for system. In this fig whole face is down as shown so its not considered as face so it could be best gesture to system.

Fig.5 Case 3

Case 4: This fig shows one side face which has probablity to cosider it in frame only 50% chance to detect it as face as shown in fig 6. It could be alternative to gesture .So its not considered as face.

Fig.6 Case 4

Case 5: Fig shows that to recognize the face in image 100 % face is shown to system. In this whole face is shown so it is considered as face not as gesture. It is best image to recognize the face.

Fig.7 Case 5

After checking the results we come to conclusion that it is not necessary to provide gesture just user at unusual condition has to move away his/her face from the frame or camera after some slot of time.

Acknowlegement

It gives us great pleasure to acknowledge our topic titled: **Adaptive Intelligent Authentication System For Highly Confidential Data (AIAS)**. We are interested in the field of Artificial Intelligence, security and Adaptive systems. With deep sense of gratitude we would like to thanks all the people who have lit our path with their kind guidance.

We are very grateful to these intellectuals who did their best to help during our research work. It is our proud privilege to express great gratitude to, Prof (Dr). V.J. Gond Principal of Late G.N Sapkal College of Engineering, We remain indebted to Prof. N.R. Wankhade, HOD Computer Engineering. And the special gratitude goes to our project coordinator and project guide Prof. B. R. Nandwalkar. We are also thankful to our parents for providing their wishful support for completion of our work successfully. And lastly we are thankful to all friends and the people who are directly or indirectly related to our project work.

References

[1]. Kamal Nasrollahi and Thomas B. Moeslund, "Haar-like features for robust real-time face recognition". *Image Processing (ICIP), 2013 20th IEEE International Conference, Melbourne, VIC, 3073 - 3077 INSPEC Accession Number: 14112798, 15-18 Sept. 2013.*

[2]. Prof.Padma Nimbhore, Abhilash Shah, Sagar Mantri, Ninad Kumthekar, Sumit Thakre "Dynamic Hand Gesture Recognition Using Real Time Motion Template Gradients". *IEEE Sponsored International Conference On Empowering Emerging Trends In Computer, Information Technology & Bioinformatics International Journal of Computer, Information Technology & Bioinformatics (IJCITB) ISSN: 2278-7593, Volume-2, Issue2.*

[3]. Ashish kumar Dewangan, Majid Ahmad Siddhiqui "Human Identification and Verification Using Iris Recognition by Calculating Hamming Distance", *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.*

[4]. Soweon Yoon, Jianjiang Feng and Anil K. Jain "Altered Fingerprints: Analysis and Detection". *IEEE transactions on pattern analysis and machine intelligence, vol. 34, no. 3, march 2012.*

[5]. Zhong Yang, Yi Li, Weidong Chen, Yang Zhen, Dynamic Hand Gesture Recognition using Hidden Markov Models, *Computer Science & Education (ICCSE), 2012 7th International Conference on Melbourne, VIC.*

[6]. Nayana P B, Sanjeev Kubakaddi," Implentation of Hand Gesture Recognition Technique for HCI Using Open CV", PG Scholar, Electronics & communication department, Reva ITM, Bangalore-64, CEO, ITIE Knowledge Solutions, Bangalore-10. *International Journal of Recent Development in Engineering and Technology Website: www.ijrdet.com ISSN 2347 - Volume 2, Issue 5, May 2014.*

[7]. Meenakshi Panwar and Pawan Singh Mehra , ―Hand Gesture Recognition for Human Computer Interaction‖, *in Proceedings of IEEE International Conference on Image Information Processing(ICIIP 2011), Waknaghat, India, November 2011.*

