

Advanced Authentication System Using Graphical Password

Wanjari Nilima ^{#1}, Aher Vaishnavi ^{*2}, Pagare Sharmila ^{#3} Kulkarni Hema ^{*4}

[#]Department of Computer Engineering,
JESITMR, Nashik, India

Abstract— In this project, the proposed system is an Advanced Authentication System for providing more security to highly confidential data. The aim of this system is to provide the user with the more secure authentication based on condition. Here, Advanced Authentication System is adaptive and can be properly used for data security purpose. We are using graphical password for normal authentication but in threat we are using gesture detection.

Keywords— Graphical Password, Gesture Detection, Haar Cascade, OpenCV, Viola Johns.

I. INTRODUCTION

The aim of the proposed system is to provide the user with the more secure authentication based on condition. In this project, the proposed system is an Advanced Authentication System for providing more security to highly confidential data. Normally, authentication is based on the biometric thumb, Finger detection, palm detection or Eris scan. They are considered as the most secure for authentication but this system is providing Graphical password system based on Knowledge based system. In the unusual condition there is a high chance where authorities may be forced to give access. Here, Advanced Authentication System is adaptive and can be properly used for data security purpose. The proposed system is using graphical password for normal authentication but in threat it is using gesture detection.

II. LITRETURE REVIEW

In existing systems, it was really challenging to detect face. It was more difficult when our input face image is noisy or very low resolution. There are many problems in feature extraction and face recognition system. In our proposed system, Haar like features are used, which is mainly used for object detection and face recognition. The proposed system is real time, robust, effective and simple. Previous systems have used OpenCV for real time. OpenCV's recognition rate is fast and the requirement rate is low. Hence, OpenCV is good option for choosing as gesture detection technique. Instead of biometric system, we are using Graphical Password Technique. In today's security systems, knowledge-based schemes are used for user authentication. Biometrics can be used for user identification but one problem with the systems is the difficult between impostor pass rate and false alarm rate. Many Biometric systems require devices and some can be difficult to use. After referring various papers and techniques there are number of algorithms for authentication of right person but there may be the unusual

condition where confidential data may be lost and hence there should be some system where access should be given to right person at right situation.

III. EXISTING SYSTEM

Referring to the papers and technology used for authentication, most of the system uses biometric technologies there are five types of technologies:

1. Facial
2. Eris Scan
3. PIN Code
4. Thumb Detection
5. Palm Detection

In addition, many biometric systems require specialized devices, and some can be unpleasant to use. For example, In case of Eris scan eye structure scanned and access is given but it has a various disadvantages like pupils may spread due to the presence of extra light factors if user is using lenses or spectacles then system may fail. All the above techniques are best for authentication purpose but there is a common drawback for all the systems. Though these systems are giving authentication by right person but may not be at right situation. So, unauthorized person may force or harm the person to get access to the system.

IV. PROPOSED SYSTEM

So, There should be some techniques to handle these kind of situation .The proposed system are providing solution for these kind of problems. The proposed system is Advanced Authentication System (AAS). For understanding the situation, the proposed system is using gesture to inform system about unusual condition. We have to make system intelligent enough to check right person along with right situation. According to the situation it will react intelligently and we are also using graphical password to it. Most token-based authentication systems also used knowledge-based authentication to prevent theft or loss of the token. An example is ATM authentication, which requires a combination and a PIN. The knowledge based techniques are currently the most frequently used method for user authentication.

A. Password Authentication Methods:

1. Token based authentication method.
2. Biometric based authentication method.
3. Knowledge based authentication method.
 - Recognition method.
 - Recall method.

B. Dhamiga and Perrig Method :

Dhamiga and Perrig proposed a technique called “Déjà vu” based on human ability to remember previously seen images. It is a recognition based method. User has to choose few images from a set of stored abstract images. User has to execute these same images at login time. These images are created using Andrej Bauer’s Random Art. They showed 90% success proportion using “Déjà vu” scheme.

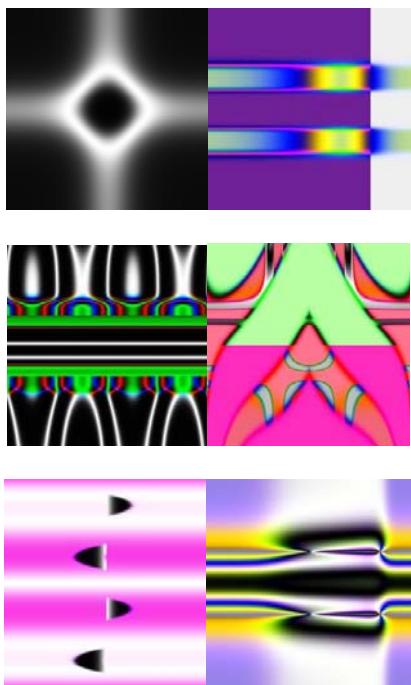


Fig.1 Example of Random Art Images

V. SYSTEM ARCHITECTURE

For informing the system about the unusual condition user at a victim's system has to give gesture with graphical password which helps the system to understand and behave accordingly to the situation. At the time, an attacker may be busy in accessing the data which is actually a fake data he assumed to be true and with the help of video streams and notification at remote location situation can be in control. If there is no unusual condition it means there is no threat then simply user have to give graphical password to access database.

A. Description of Module :

1. Login :

It is an important part to have a login facility for an application due to the important factor of security. As every application contains database, so data related to every user can be stored. Login helps to trace out the user who in case tries to make any malicious activity within the application.

2. Session Management:

In usual/unusual condition user will have to choose few images from a set of stored abstract images. The user has to execute same images at login time with ID for accessing a confidential data. When again the ID and password will generate, it will scan against the template and again new ID and password is created. When the old and current will match then authentication is provided. As our first module is graphical password based.

The work of the proposed system is just to process and check the generated which the authorized person can easily access the data without giving gesture.

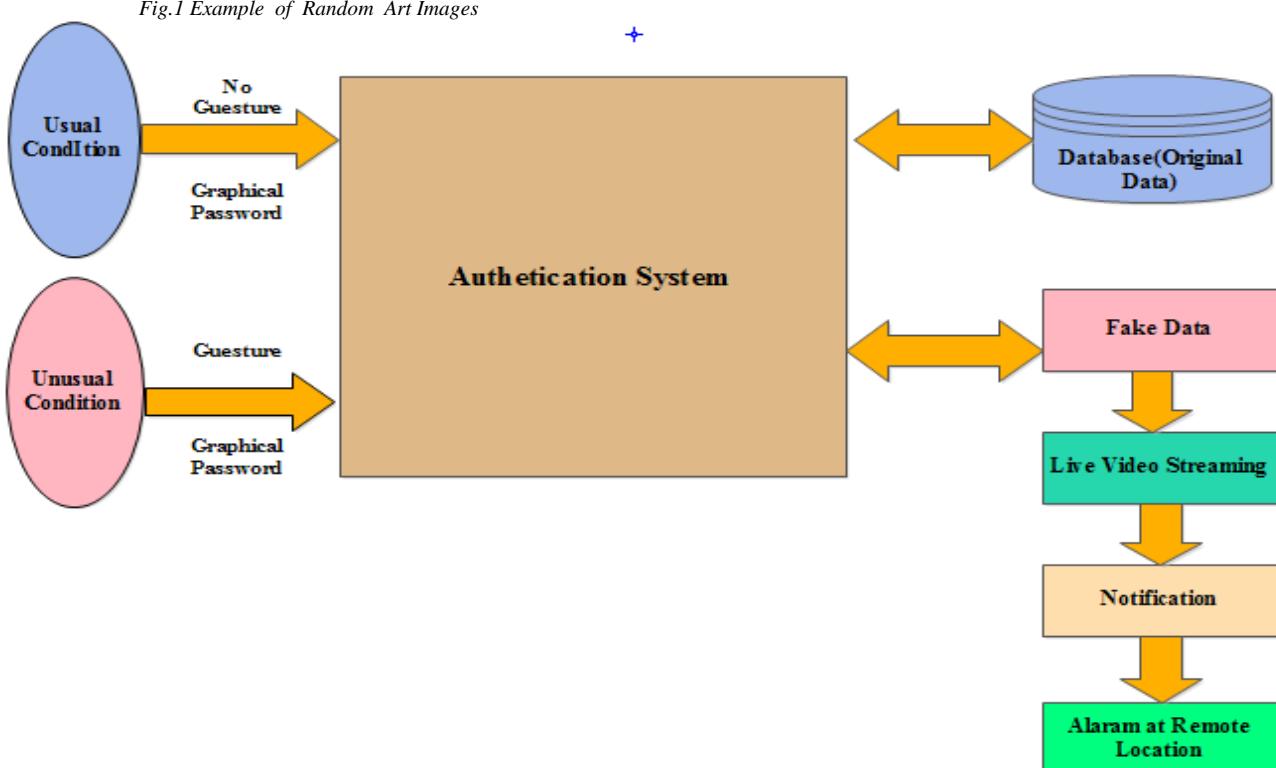


Fig. 2. System Architecture

VI. ALGORITHMS

The proposed system contains the flow which is based on two conditions:

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

In usual condition authorized user will give graphical password for accessing data. In which the authorized person easily access data without giving gesture.

A. Gesture Detection:

There are various algorithms on gesture detection. There is need to detect gesture at real time as need of the system and to detect gesture at real time, using open CV is better option.

In proposed system, Haar like feature detection algorithm is used.

B. Viola Jones Algorithm:

Viola Jones implemented an algorithm which utilized Haar like features for facial feature detection instead of analyzing the pixels. These features are digital image features used in object recognition. It is considered as an adjacent rectangular regions. The position of these rectangles is relative to a detection window that acts like a bounding box to the target object. The detection part of the Viola Jones object , a window of the target size is moved on the input image. Each part of the image the Haar like feature is calculated. This difference is compared to a learned threshold that separates non-objects from objects.

C. Steps for algorithms:

1. The first step in facial feature is detecting the face. This requires analyzing the entire image.
2. The second step is using the isolated face(s) to detect each feature. The result is shown in Fig 1. Since each the portion of the image used to detect a feature is much smaller than that of the whole image, detection of all three facial images, a frame rate of 3 frames per second was achieved. Since a frame rate of 5 frames per second was achieved in facial detection only by using the given requirement, recognition provides a tremendous increase in efficiency in facial feature.

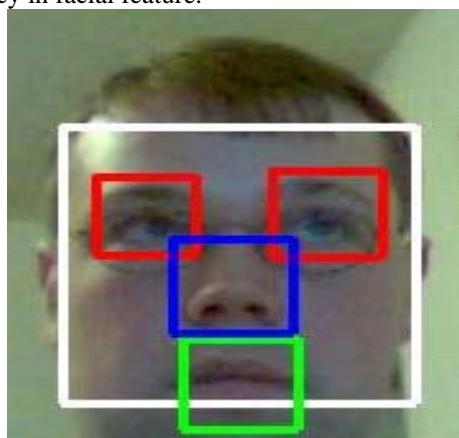


Fig.1 Output of Whole Image

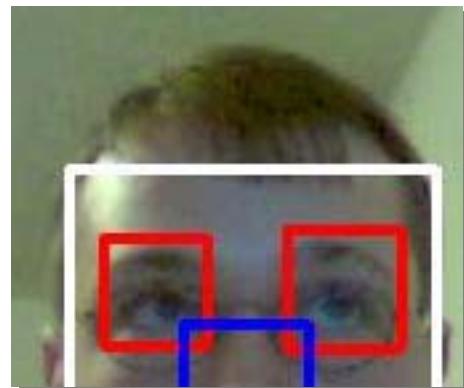


Fig.2 Output of Desired Image

Thus, we come to conclusion to use only extracted features of the image to scan two eyes, half nose and forehead as per the project need.

VII. CONCLUSION:

In this way, we have completed the design part of the project with the requirement specification modules of the project are designed and are well studied in order to fulfill the requirements of the project. The completion of partial report is being completed with full hard work and complete support and guidance of our guide and project plan is made to ensure the proper planning of the project.

REFERENCES

- [1] Mamta S.Kala, " Real Time Face Detection And Tracking Using OpenCV ", International Journal of Soft Computing and Artificial Intelligence, ISSN: 2321-404X, Volume-2, Issue-1, May-2014
- [2] Harshith.C, Karthik.R.Shastry, Manoj Ravindran, M.V.V.N.S Srikanth, Naveen Lakshmikanth,"Survey On Various Gesture Recognition Techniques For Interfacing Machines Based On Ambient Intelligence", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.
- [3] R.V.Sudhakar, A. Mruthyunjayam, D. SugunaKuamari, M. Ravi Kumar, B.V.S. Ramesh Babu "Improving Login Authorization by Providing Graphical Password (Security)", International Journal of Engineering Research and Application ISSN: 2248-9622, Vol. 3, Issue 6, Nov-Dec 2013, pp.484-489
- [4] Swapnil Athavale ,Mona Deshmukh , " Dynamic Hand Gesture Recognition for Human Computer interaction" , International Journal of Engineering Research and General Science Volume 2, Issue 2, Feb-Mar 2014,ISSN 2091-2730
- [5] Varun Jasuja, Mr. Marish Singla,Mr. Rajesh, "Multiple Face Detection & Recognition Using Principal Component Analysis Algorithm" International Journal of Engineering Research and General Science Volume 2, Issue 2, Feb-Mar 2014 ISSN 2091-2730
- [6] Giriraj R. Mulay, Anil S. Kale, Ganesh S. Mate, Ravindra P. Tupe " Adaptive Intelligent Authentication System (AIAS) ", International Journal for Research in Engineering Application & Management (IJREAM) Vol-01, Issue 01, APR 2015.
- [7] Sajjad Ur Rahman, Zeenat froze, Mohammed Tareq, " Hand Gesture Recognition Techniques For Human Computer Interaction Using OpenCv", International Journal of Scientific and Research Publications, Volume 4, Issue 12, December 2014 1 ISSN 2250-3153
- [8] Farnaz Towhidi, Maslin Masrom, " A Survey on Recognition-Based Graphical User Authentication Algorithms", International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009.
- [9] Geeta M. Rane, " Graphical Password Authentication: Methods and Schemes", International Journal of Trend in Research and Development, Volume 2(5), Sep - Oct 2015 . ISSN 2394-9333
- [10] 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.