International Journal of Technology and Engineering System (IJTES)
Vol 7. No.3 2015 Pp. 224-229

available at : www.ijcns.com
ISSN: 0976-1345

SECURED LOGIN FOR GMAIL USING PATTERN CLASSIFIER WITH VOICE RECOGNITION

S.LAVANYA[1] M.ANUPRIYA[2] S.VINODHINI[3], J.GOBINATH[4,]
Bachelor of Engineering, Dept of IT
, Assistant Professor, Dept of CSE
Rajiv Gandhi College of Engineering, Chennai, India
lavuit93@gmail.com[1] anupriya.m12@gmail.com[2] vino1293svk@gmail.com[3]
gobirgce@gmail.com[*]

ABSTRACT

Fractal detection and recognition is a unique process for identifying every human being. This concept is more effective interms of authentication into the service. This module permits us to response in building each and every image sets followed by the measure of similarity metrics and models comparison. In the proposed system achieves efficient similarity matching and reducing storage utilization of a method called pattern classifiers that has been implemented. Pattern classifiers are used in this system such as keyword, URL for data check, tag construction and keyword identity etc. Moreover, the system involves voice recognition process to convert voice to text message in order to reduce the user complication. The overall modules of the proposed system are implemented in the Gmail server via legal authentication.

Index terms: Pattern Classifiers, Fractal Detection, Voice Recognition, URL

1.INTRODUCTION

Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. The scope of the project is the process of improving security to the data by means of fractal detection in terms of implementing a framework in Gmail. Pattern classifiers and spamming the mail with unwanted keyword is also a part of the project. High effective authentication with the purpose of log on to the email service securely and efficient spamming are taken into

consideration.Authentication in the form of fractal detection and recognition after contour detection of the face using the image of the user is introduced. Pattern classifiers such as Keywords and URL's for data check, tag construction and keyword identity, automatic readings of mails are the concepts used in this system.

II.RELATED WORK

Security Evaluation of Pattern Classifiers under Attack [1] evaluating at design phase the security of pattern classifiers namely, the performance degradation under potential attacks they may incur during operation. A framework for empirical evaluation of classifier security that formalizes and generalizes the main ideas proposed in

the literature, and give examples of its use in three real applications. Reported results show that security evaluation can provide a

Representation of data is done using a vector space model. Clustering is the technique used for data reduction. Robustness of multimodal biometric fusion methods against spoof attacks [5] consists different approach to spam detection is based on the behavior of email senders. A learning approach to spam sender detection based on features extracted from social networks constructed from email exchange logs.

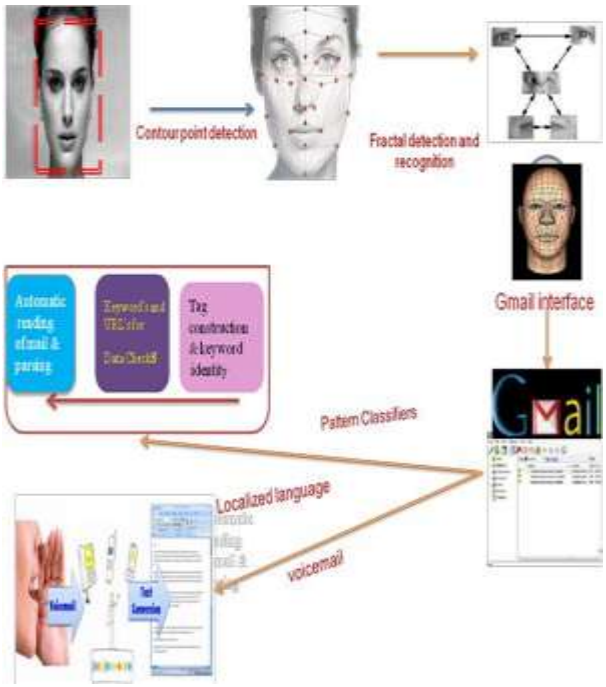
SECURITY OF LEARNING ALGORITHMS

While developing or even classifying techniques for recognizing faces, we can look at them from different perspectives. Original pattern should be also transformed into some representation that can be easily manipulated programmatically. This step depends on the structure of the data set. Classification: matching data based on measurements similarities with other patterns, mostly via an artificial neural network. Machine learning techniques have not been originally designed to cope with intelligent and adaptive ad varsities that can manipulate input data to subvert the learning process.

with intelligent and adaptive ad varsities that can manipulate input data to subvert the learning process.

III.SYSTEM DESIGN

System Design involves identification of classes their relationship as well as their collaboration. In objector, classes are divided into entity classes and control classes. The Computer Aided Software Engineering (CASE) tools that are available commercially do not provide any assistance in this transition. CASE tools take advantage of Meta modeling that are helpful only after the construction of the class diagram. In the FUSION method some object-oriented approach likes Object Modeling Technique (OMT), Classes, and Responsibilities. Collaborators (CRC), etc, are used. Objector used the term ”agents” to represent some of the hardware and software system. In Fusion method, there is no requirement phase, where a user will supply the initial requirement document. Any software project is worked out by both the analyst and the designer.



The analyst creates the user case diagram. The designer creates the class diagram. But the designer can do this only after the analyst creates the use case diagram. Once the design is over, it is essential to decide which software is suitable for the application.

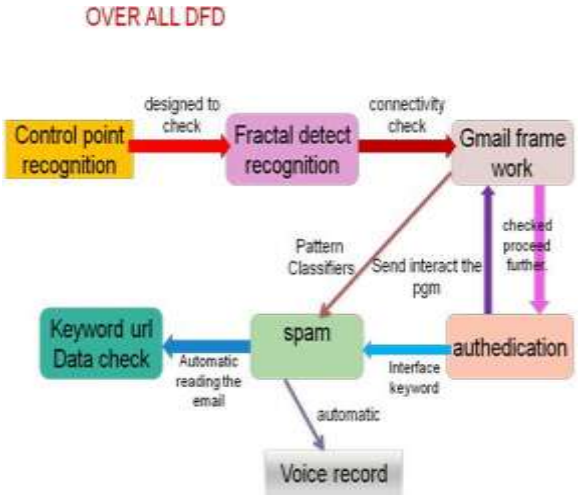


Fig.2. Overall DFD

1. PROPOSED SYSTEM

The systems high effective authentication with the purpose of log on to the email service securely and efficient spamming are taken into consideration. Authentication in the form of fractal detection and recognition after contour detection of the face using the image of the user is introduced. Since fractal detection and recognition is an unique method to identify every human being, this concept is more effective in terms of authenticating into the service. Pattern classifiers such as Keywords and url's for data check, tag construction and keyword identity, automatic reading of mails are the concepts used in this system. Administrator of the email service uses the pattern classifiers and maintains a repository to filter out spam domains and keywords. Hence this perception spams the frequent surplus mails from same domain with different mail id's. Automatic reading of mails to examine the spammed keyword is an intriguing conception introduced in this system to overcome many flaws in case of spam filtering. Hence the authentication by means of fractal recognition and pattern classifier based spam filtering in the email service turn this proposed system more thriving and thus overcomes the drawbacks of existing system.

2.FRACTAL CODE BASED FACE RECOGNITION TECHNIQUE

It is shown that candidate images of face recognition system could be recognized, efficiently, using interdependence of pixels arising from fractal codes (IFS) of images. The interdependence of the pixels is inherent within the fractal code in the form of chain of pixels. The mathematical principal behind the application of fractal image codes for recognition is, an Image Xf can be represented as,

$$Xf = A \times Xf + B$$

which A and B are fractal parameters of image Xf. Different fractal codes can be presented for any arbitrary image. With the definition of a fractal Transformation.

$$T(X) = A\,(X - Xf) + Xf$$

3.BRUTE FORCE STRING MATCH ALGORITHM

ALGORITHM *BruteForceStringMatch*$(T[0..n-1],\ P[0..m-1])$
```
//Implements brute-force string matching
//Input: An array T[0..n − 1] of n characters representing a text and
//       an array P[0..m − 1] of m characters representing a pattern
//Output: The index of the first character in the text that starts a
//        matching substring or −1 if the search is unsuccessful
for i ← 0 to n − m do
    j ← 0
    while j < m and P[j] = T[i + j] do
        j ← j + 1
    if j = m return i
return −1
```

IV.SYSTEM IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned.

1. *Contour Point Facial Recognition Module*

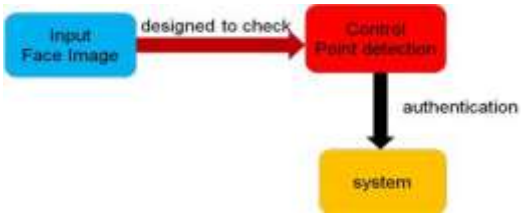


Fig.3. Contour Point Facial Recognition

A contour point is a way of representing a three-dimensional surface on a flat, two-dimensional surface. The active contour method can be used to determine face features in a picture. This module is designed to check the input face using contour point facial recognition that is to be used as an authentication for the system.

2. *Gmail Connectivity Check Module*

The Gmail SMTP server settings for sending mail through Gmail from any email program. A programming interface has been designed to interact with the Gmail server. In this module, the connection establishment has been checked to proceed further.

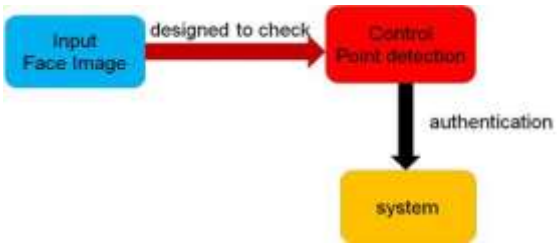


Fig.4. Gmail connectivity check module

3. *Gmail Authentication Module*

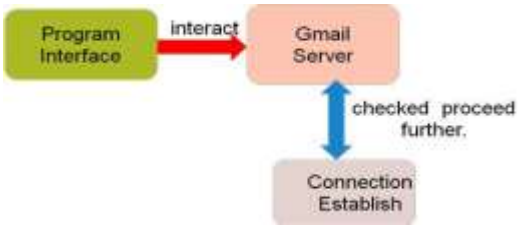


Fig.5. Gmail Authentication

Gmail authentication is a way to ensure that an email provider will be able to recognize the sender of an incoming message and fight spam and abuse. You can use authentication data to verify the source of any message that you receive. The face that has been recognised using the contour point facial recognition is used to authenticate into the Gmail via the programming interface. The user can utilize the smart camera's to recognise their face in order to authenticate into the system.

4.Spam Keywords Append Module

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. In this module, the keywords that are considered as spam on user's perspective are appended in the interface.

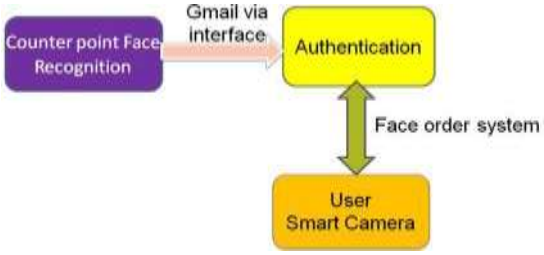


Fig.6. Spam Keywords

5. *Spam filtering-apply rule*

Spam is most often considered to be electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. A spam filter is a program that is used to detect unsolicited and unwanted email and prevent those messages from getting to a user's inbox. In this module, spam filter checks all incoming emails to your email accounts against mail filter rules.

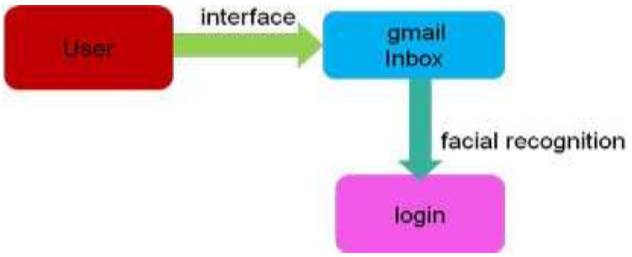


Fig.7. Spam Filtering

6. *Automatic Voice Record Module*

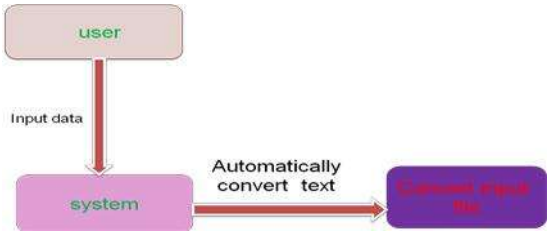


Fig.8. Automatic Voice Record

In this module, the person's voice is inputted which has been converted as text in the mail. Automatic voice will be recorded and stored in the database. The quality of machine audio transcript is high and mostly depends on original file sound quality.

V.EVALUATION RESULT

The following screen shots illustrates the login page of the application followed by the authentication process which results in the connectivity check page confirming the server connection. Fig. 11. Shows the mail box. The next figure enables the user to customize the spam keywords.

Fig.9. Login page

Fig.10. Connectivity Check

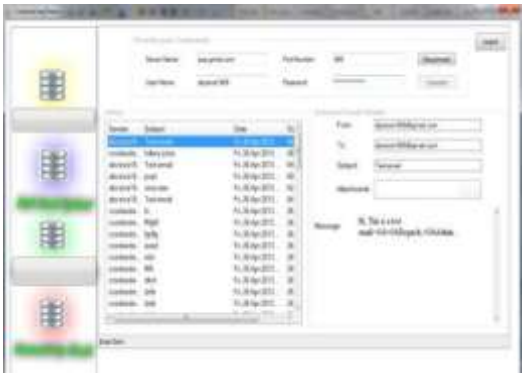


Fig.11. Test Mail

Fig.12. Adding Spam Information

VI. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we have introduced a new method for high effective authentication with the purpose of log on to the email service securely and efficient spamming. Pattern classifiers such as Keywords and URL's for data check, tag construction and keyword identity, automatic reading of mails is the concepts used in this system.Every aspect of security in terms of data is discussed in this project but the user's perspective is not discussed. So, in the future enhancement the user perspective like forgetting the password will be implemented.

REFERENCES

[1] Security Evaluation of Pattern Classifiers under Attack Battista Biggio, Member, IEEE , Giorgio Fumera, Member, IEEE , and Fabio Roli, Fellow, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 26, NO. 4, APRIL 2014.

[2] B. Biggio, Z. Akhtar, G. Fumera, G.L. Marcialis, and F. Roli, "Security Evaluation of Biometric Authentication Systems under Real Spoofing Attacks," IET Biometrics, vol. 1, no. 1, pp. 11-24, 2012

[3] B. Biggio, B. Nelson, and P. Laskov, "Poisoning Attacks against Support Vector Machines," Proc. 29th Int'l Conf. Machine Learning, 2012.

[4] Dagstuhl Perspectives Workshop Mach. Learning Methods for Computer Sec., http://www.dagstuhl.de/12371/, 2012.

[5] B. Biggio, G. Fumera, and F. Roli, "Design of Robust Classifiers for Adversarial Environments," Proc. IEEE Int'l Conf. Systems, Man, and Cybernetics, pp. 977-982, 2011.

[6] B.Biggio, I.Corona, G. Fumera, G.Giacinto, and F. Roli, "Bagging Classifiers for Fighting Poisoning Attacks in Adversarial Environments," Proc. 10th Int'l Workshop Multiple Classifier Systems, pp. 350-359, 2011.

[7] P. Johnson, B. Tan, and S. Schuckers, "Multimodal Fusion Vulnerability to Non-Zero Effort (Spoof) Imposters," Proc. IEEE Int'l Workshop Information Forensics and Security, pp. 1-5, 2010

[8] R.N. Rodrigues, L.L. Ling, and V. Govindaraju, "Robustness of Multimodal Biometric Fusion Methods against Spoof Attacks," J. Visual Languages and Computing, vol. 20, no. 3, pp. 169-179, 2009.

[9] A.M. Narasimha murthy and L.I. Kuncheva, "A Framework for Generating Data to Simulate Changing Environments," Proc. 25th Conf. Proc. the 25th IASTED Int'l Multi-Conf.: Artificial Intelligence and Applications, pp. 415-420, 2007.

[10] D. Lowd and C. Meek, "Good Word Attacks on Statistical Spam Filters," Proc. Second Conf. Email and Anti-Spam, 2005.