IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Face Recognized Mail Accessor with Pattern Based Spam Filtering

E. Evangelin Jeni[1], S. Jeyalaximi[2]

[1]M.E, Computer Science and Engineering, SMK Fomra Institute of Technology, Kelambakkam, Chennai, Tamil Nadu, India

[2]Assistant Professor, Computer Science and Engineering, SMK Fomra Institute of Technology, Kelambakkam, Chennai, Tamil Nadu, India

Abstract

High effective authentication with the purpose of log on to the email service securely and efficient spamming are taken into consideration. Normal authentication for logging into the email service by means of username and password characters are applicable in the existing system. But it is not secure because if anyone knows the password means they can access the mail. In proposed system, 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. Spam mail id and keyword filtering are the methods used in the existing system. Domain and url based spam filtering are the filtering techniques used in the proposed system.

Keywords: *Pattern Classification, Biometric Authentication, Spam Filtering, Face Recognition.*

1. INTRODUCTION

A face recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database.

Pattern classification systems based on machine learning algorithms are commonly used in security-related applications like biometric authentication, network intrusion detection, and spam filtering, to discriminate between a "legitimate" and a "malicious" pattern class (e.g., legitimate and spam emails). Well known examples of attacks against pattern classifiers are: submitting a fake biometric trait to a biometric authentication system (*spoofing* attack) [1], [2]; modifying network packets belonging to intrusive traffic to evade intrusion detection systems [3]; manipulating the content of spam emails to get them past spam filters (e.g., by misspelling common spam words to avoid their detection) [4]–[6].

Spam contents in the web are not only utilizes valuable resources inside the web but can also mislead the users to unsolicited websites and award undeserved search engine rankings to spammer's campaign websites. There is open research area in identifying the individual person's emails by manipulating through an automated supervised machine learning solution which utilizes web navigation behavior to detect the possible spams. The existing approach needs an effective representation of e-mail (i.e., e-mail abstraction). Large sets of reported spams has to be stored in the known spam database, the storage size of e-mail abstraction should be small. Moreover, the email abstraction should capture the near-duplicate phenomenon of spams, and should avoid accidental deletion of nonspam e-mails.

2. MOTIVATIONS

Major issue of the existing system is identification of patterns to avoid spams. Nowadays, spams are considered as one of the major technical problem for most of the users and we don't have proper solution in manipulating the following key issues like,

- Email scanning before it's read by the users
- Blocking the domain irrespective of the users email id
- Keyword based blocking by monitoring the subjects
- Blocking the users url

Password visualizing or Password trap is one of the major flaws in the available systems that too for the public domains.

3. GMAIL FRAMEWORK ARCHITECTURE

3.1 Contour Point Facial Recognition

A facial recognition system is a computer application forautomatically identifying or verifying a pers on from a digital image or a video frame from a video source. 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 method is designed to check the input face using contour point facial recognition that is to be used as an authentication for the system.

3.2 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. 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.

3.3 Gmail Connectivity Check

Gmail is a free, advertising-supported email service provided by Google. Users may access Gmail as secure webmail, as well as via POP3 or IMAP4 protocols. The Gmail SMTP server settings for sending mail through Gmail from any email program. Gmail SMTP server address: smtp.gmail.com. A programming interface has been designed to interact with the Gmail server. In this method, the connection establishment has been checked to proceed further.

3.4 Gmail Inbox View

An inbox is the main folder that your incoming mail get stored in. When you check your mail through a webmail interface or use a program like Gmail, each downloaded message gets stored in your inbox. After the completion of authentication process this module is executed. In this method, the user will be able to view the Gmail inbox through the programming interface once after logging in into the system by facial recognition.

3.5 Spam Keywords Append

In text editing, a keyword is an index entry that identifies a specific record or document. 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 method, the keywords that are considered as spam on user's perspective are appended in the interface.

3.6 Spam Detection

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 method, spam filter checks all incoming emails to your email accounts against mail filter rules.

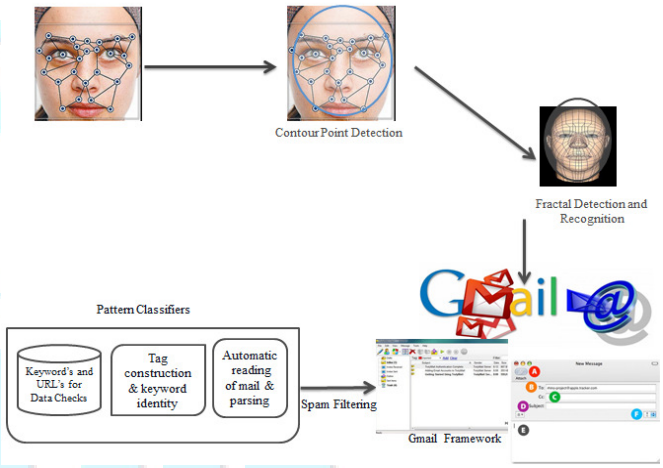

Fig. 1 Gmail Framework Architecture.

4. CONCLUSIONS

In this paper a new method for high effective authentication with the purpose of log on to the email service securely and efficient spamming is introduced. 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 paper.

5. FUTURE ENHANCEMENT

Every aspect of security in terms of data is discussed in this paper but the user's perspective is not discussed. So, in the future enhancement the user perspective like forgetting the password will be implemented. Voice recognition concept can also be implemented to make the system more user interactive. The future work will be devoted to develop techniques for simulating attacks for different applications.

REFERENCES

[1] R. N. Rodrigues, L. L. Ling, and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks," J. Vis. Lang. Comput., vol. 20, no. 3, pp. 169–179, 2009.

[2] P. Johnson, B. Tan, and S. Schuckers, "Multimodal fusion vulnerability to non-zero effort (spoof) imposters," in IEEE Int'l Workshop on Inf. Forensics and Security, 2010, pp. 1–5.

[3] P. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee, "Polymorphic blending attacks," in Proc. 15th Conf. on USENIX Security Symp. CA, USA: USENIX Association, 2006.