

Fractal Techniques for Human Face Recognized Mail Accessor with Pattern Based Spam Filtering

A. Ramyaa¹ C. Thirumalaiselvan²

¹M.E. Student ²Assistant Professor

^{1,2}Department of Computer Science & Engineering

^{1,2}K.S.R College of Engineering, Tiruchengode, 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.

Key words: Pattern classification, fractal detection, contour point detection, and spam filtering

I. INTRODUCTION

Electronic mail, most commonly referred to as email or email. It is a method of exchanging digital messages from a sender to one or more receivers. Gmail is a free email service produced by Google. Users may access Gmail as reliable webmail via POP3 or IMAP4 protocols. Spam can be defined as unsolicited email for a recipient or any email that the user do not wanted to have in his inbox. It is also defined as “Internet Spam is one or more unwanted messages, sent as a part of larger set of messages, all having considerably similar content.” There are significant problems from the spam mails, wastage of network resources, delay, destruction to the PC’s & laptops due to viruses & the ethical issues such as the spam emails advertising pornographic sites which are harmful to the young generations [1].

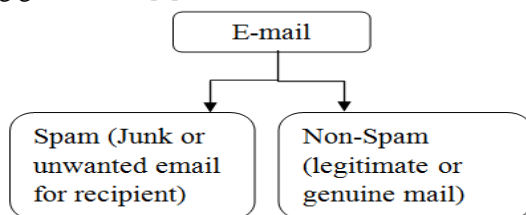


Fig. 1: Email types

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. Most of the research in anti-spam filtering focuses on the origin of spam content, only a few have investigated the identification of spam content on the web, and filtering mechanism. 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 spam. The existing approaches need an effective representation of e-mail. Large sets of reported spam has to be stored in the known spam database, the storage size of email abstraction should be small. Moreover, the email abstraction should capture the near-duplicate phenomenon of spam, and should avoid accidental deletion of non-spam e-mails.

Password hijacking or Password exposure is one of the major problem in the area of Password the scenarios. We don’t have proper system for this major issue. Multimodal biometric systems for personal identity recognition are more popular in the past few years. It has been shown that combining information coming from different biometric traits can overcome the limits and the weaknesses inherent in every individual biometric, resulting in a higher accuracy. Moreover, it is commonly believed that multimodal systems also improve security against spoofing attacks, which consist of claiming a false identity and submitting at least one fake biometric trait to the system.

II. RELATED WORKS

Here we analyzed previous work, highlighting the concepts that will be utilized in our system. Message passing through emails is one the well-known way of today’s world since it is more effective and fast than any other sources. Authentication is the major part often involves verifying the validity of at least one form of identifications of the users. Normally authentication for logging in to the Gmail service by means of username and password characters is applicable in the existing system. Security type of authentication such as logging in to the Gmail service using the secret code received to the mobile device of the user is also applicable. This in turn less effectual since anybody who accesses the user’s mobile can log on to the service or there is no option in case of mobile theft. Spam is a typical message passing that floods the Internet with many copies of the same message, which tried to force the message on people who would not otherwise choose to receive it. Spam keyword filtering is the way used in existing system to get rid of spam emails. Frequent mails from a mail id can be spammed if it is tested against spam filter but the domain cannot be filtered under the spam filter. Hence any number of email id can be created by the spammers to send spam mail under the same domain. Automatic email content examining and spamming is not possible. Many a time the concept of spamming is false positive in this system.

In [1] Pattern classification method used in biometric authentication system, network intrusion detection system, and spam filtering system. They evaluated security of pattern classifiers, such as the performance degradation under potential attacks they may incur during operation. They developed a frame work and that used in three application examples, such as spam filtering system,

biometric authentication system, and network intrusion detection system. Fogla, M. Sharif, R. Perdisci, O. Kolesnikov, and W. Lee[2] discussed their initial research efforts focused on the detection of malicious insiders who exploit internal organizational web servers. The objective of the research is to apply lessons learned in network monitoring domains and enterprise log management to investigate various approaches for detecting insider threat activities using standardized tools and a common event expression framework. The author is emphasizing insider threat detection in network monitoring domain. Scanning through the web server log and identify the threat is the main factor. Here, multiple events and single events from multiple hosts and single hosts is identified. In [3], they extract spam/non-spam email and detect the spam email efficiently. Here representation of data is done using a vector space model and clustering is the technique used for data reduction. In this paper an email clustering method is proposed and implemented to efficient detects the spam mails. The BIRCH clustering, decisions made without scanning the whole data & BIRCH utilizes local information (each clustering decision is made without scanning all data points). BIRCH is a better clustering algorithm requiring a single scan of the entire data set thus saving time. So, it cannot work in any other algorithm. In this work [4], they present the design and implementation of Pyramid-like Face Detection (PFAD), which is a real-time face detection system constructed on general embedded devices. It is motivated by the observation that the computation overhead increases proportionally to its pixel manipulation-FAD propose a hierarchical approach to shift the complex computation to the promising regions. They introduce the hierarchical framework for face detection on embedded smart camera briefly. And focus on tackling the challenging issues in constructing the hierarchical scheme.

III. PROPOSED SYSTEM

In our proposed system, high effective authentication with the purpose of log on to the Gmail service securely and efficient spamming are taken into consideration .Here 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 is 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. 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.

IV. SYSTEM ARCHITECTURE

System architecture is the conceptual model that defines the structure and/or behavior of the system. It provides a way in which products can be procured, systems can be developed an architectural overview of the overall system. The system architecture for the proposed system is given in fig. 2. The above architecture diagram Fig. 2 shows that the active contour method can be used to determine face features in a picture. To check the input face using contour point facial recognition that is to be used as an authentication for the system. The face that has been recognized using the contour point facial recognition is used to authenticate into the Gmail via the programming interface.

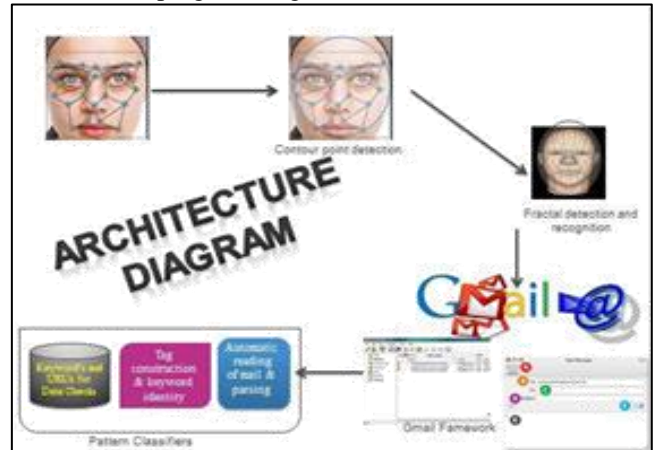


Fig. 2: Architecture diagram

The user can utilize the smart camera's to recognize their face in order to authenticate into the system. The keywords that are considered as spam on user's perspective are appended in the interface. The spam keywords will be stored in repository. It can be used to reject the unwanted e-mails. The user can be able to view the Gmail inbox through the programming interface once after logging in into the system by facial recognition. 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. Spam filter checks all incoming emails to your email accounts against mail filter rules.

A. Objective:

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 reading of mails are the concepts used in this system.

V. FACE RECOGNITION BASED ON FRACTAL AND CONTOUR IMAGE

Human face recognition is an important area in the biometrics field. It has been an active area of research for many years. Human face is a biometric form. Biometrics are a set of measurable physiological and/or behavioral characteristic properties of the human body that can be used to infer a person's identity[5]. One of the first step of the face recognition is to detect and extract face from an image.

There are many face detection algorithms. These algorithms are mainly classified into four. Those are

- Knowledge based methods
- Feature invariant approaches
- Template matching methods
- Appearance-based methods.

Knowledge-based methods use a set of rules that developed from what humans know about the appearance of a face. Feature invariant approaches use structural features that are invariant to changes in pose, expression. Template matching methods use a set patterns representative of the face, which are then correlated with the input image. Appearance-based methods perform face detection using models or templates learnt from a set of representative training images.

VI. PATTERN BASED SPAM DETECTION

In pattern based spam detection, here filtering spam mail, id, Domain and keyword also check. There are two types of spam detection are,

- Spam Keywords Append
- Spam Message Detection

A. 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.

B. Spam Message 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.

VII. NETWORK INTRUSION DETECTION USING PAYL

In network intrusion detection, When an anomalous traffic in web server. During operation, attackers submit fake identity for biometric authentication and attackers can modify the network packets is possible. So here using PAYL (PAY-Loaded) algorithms are used to give an alert message to the administrator system. It will scan the whole data, so the accuracy can achieve more effective.

VIII. 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.

IX. 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 users interactive. The future work will be devoted to develop techniques for simulating attacks for different applications.

REFERENCES

- [1] Battista Biggio, Giorgio Fumera, Fabio Roli, "Security evaluation of pattern classifiers under Attack", IEEE Transactions on Knowledge and Data Engineering, Vol.26, No. 4, April 2014.
- [2] 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.
- [3] M. Basavaraju and Dr. R. Prabhakar, "A Novel Method of Spam Mail Detection using Text Based Clustering Approach", International Journal of Computer Applications (0975 -8887) Vol.5, No.4, August 2010.
- [4] Qiang Wang, JingWu, Chengnian Long, and Bo Li, *Fellow*, "PFAD: Real-Time Face Detection Scheme on Embedded Smart Cameras", IEEE Journal on Emerging and Selected Topics In Circuits And Systems, Vol.3, No. 2, June 2013.
- [5] 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, June 2012.
- [6] 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.
- [7] K. Nandakumar, Y. Chen, S.C. Dass, and A. Jain, "Likelihood Ratio-Based Biometric Score Fusion", IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 30, No. 2, pp. 342-347, 2009
- [8] 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.
- [9] Hossein Ebrahimpour-Komleh, "Fractal Techniques for Face Recognition", A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy, Queensland University of Technology,2004.
- [10] G. L. Wittel and S. F. Wu, "On attacking statistical spam filters", in 1st Conf. on Email and Anti-Spam, CA, USA, 2010
- [11] R. O. Duda, P. E. Hart, and D. G. Stork, Pattern Classification. Wiley-Interscience Publication, 2000.
- [12] N. Dalvi, P. Domingos, Mausam, S. Sanghai, and D. Verma, "Adversarial classification", in 10th ACM SIGKDD Int'l Conf. on Knowl. Discovery and Data Mining, WA, USA, pp. 99-108, 2004.
- [13] M. Barreno, B. Nelson, R. Sears, A. D. Joseph, and J. D. Tygar, "Can machine learning be secure?", in

Proc. Symp. Inf., Computer and Commun. Sec. (ASIACCS). NY, USA: ACM, pp. 16–25, 2006.

- [14] A. A. C'ardenas and J. S. Baras, "Evaluation of classifiers: Practical considerations for security applications", in AAAI Workshop on Evaluation Methods for Machine Learning, MA, USA, 2006.
- [15] P. Laskov and R. Lippmann, "Machine learning in adversarial environments", Machine Learning, VOL. 81, pp. 115–119, 2010.
- [16] L. Huang, A. D. Joseph, B. Nelson, B. Rubinstein, and J. D. Tygar , "Adversarial machine learning", in 4th ACM Workshop on Artificial Intelligence and Security, IL, USA, pp. 43–57, 2011.

