IRJCS: International Research Journal of Computer Science
Volume 11, Issue 10, November 2024
ISSN: 2393-9842
https://www.irjcs.com/archives

Image Spam Detection through Pattern Recognition with IP Tracing Technique

S.Santhi
Assistant Professor/ Dept of CS
Vivekanandha Arts and Science College for Women
Sankari, Tamil Nadu, INDIA
sanmcappm@gmail.com
M.Mohan
Assistant Professor / Dept of CS
Swamy Vivekanandha College of Pharmacy
Tiruchengode,Tamil Nadu, INDIA
mdtech22@gmail.com

Publication History
Manuscript Reference No: IRJCS/RS/Vol.11/Issue10/NVCS10080
Research Article | Open Access | Double-Blind Peer-Reviewed
Article ID: IRJCS/RS/Vol.11/Issue10/NVCS10080
Received: 28, October 2024, Revised: 02, November 2024 | Accepted: 07 November 2024 Published Online: 10, November 2024
http://www.irjcs.com/volumes/Vol11/iss-10/01.NVCS10080.pdf
Article Citation: Santhi,Mohan(2024). Image Spam Detection through Pattern Recognition with IP Tracing Technique. IRJCS: International Research Journal of Computer Science, Volume 11, Issue 10 of 2024 pages 601-604
doi:> https://doi.org/10.26562/irjcs.2024.v1110.01
BibTeX Santhi@2024Image

Abstract: Image spam is a kind of E-mail spam where the message text of the spam is presented as a picture in an image file. The basic rationale behind image spam is difficult to detect using text spam filtering methods which is designed to detect patterns in text in the plain-text E-mail body or attachments. A new trend in email spam is the emergence of image spam. The most previous works of image spam detection focused on filtering the image spam on the client side. This proposed system considered more desirable comprehensive solution which embraces the both server side filtering and client side detection methods. The spectral clustering algorithm is introduced to similarity measure for cluster analysis of spam images to filter the attack activities of spammers and fast trace back the spam sources. The active learning algorithm is limited where the learner guides the users to label as few images as possible while maximizing the classification accuracy.

Keywords: Pattern Recognition, IP Trace back, Non Spar city, Active Learning, Image Spam hunter, Image Descriptor

I. INTRODUCTION

E-mail spam has become an epidemic problem that can negatively affect the usability of electronic mail as a communication means. Besides wasting user's time and effort to scan and delete the massive amount of junk e-mails received, it consumes network bandwidth and storage space, slows down e-mail servers, and provides a medium to distribute harmful and/or offensive content. In addition, spam reduced the network bandwidth and storage space and can slow down email servers. Spam software can also be used to distribute harmful content such as viruses, trojan horses, worms and other malicious codes. It can be a means for phishing attacks as well [9].

As a result, spam has become an area of growing concern attracting the attention of many security researchers and practitioners. Front-end filtering was the most common and easier way to reject or quarantine spam messages as early as possible at the receiving server and also most of the early anti-spam tools were static. For example using a blacklist of known spammers, a white list of good sources, or a fixed set of keywords to identify spam messages [7]. These list-based methods can substantially reduce the risk tactics and provided that lists are updated periodically, they fail to scale and to adapt to spammer's tactics. They can be defeated easily by changing the sender's address each time, intentionally misspelling words, or forging the content to bypass spam filters.

FEATURE EXTRACTION – COLOR MODELS

An RGB color space is any additive color space based on the RGB color model. A particular RGB color space is defined by the three chromaticity's of the red, green, and blue additive primaries. This module can be produced any chromaticity that is the triangle defined by those primary colors. The complete specification of an RGB color space also requires a white point chromaticity and a gamma correction curve. The RGB color model is widely used to represent digital images on most computer systems.

IP TRACE BACK

IP Trace back is a name given to any method for reliably determining the origin of a packet on the Internet. Due to the trusting nature of the IP protocol, the source IP address of a packet is not authenticated. As a result, the source address in an IP packet can be easily identified by spammers. The packets which are need not be received to continue the attack the problem of finding the source of a packet is called the IP trace back problem. IP Trace back is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. In this type of solution, gives to track the spammer origin address when server detects the image spam and then block the user account for further process.

2. LITERATURE REVIEW

Many anti-spam systems also use a combination of white lists, blacklists, and so-called grey lists that force legitimate clients to re-send messages since spammers often do not bother doing so. Other common techniques include block lists distributed via DNS that identify addresses assigned to dialup users or known open relays and challenge-response systems that automatically build white lists. Most systems such as Mail Avenger, Spam Assassin, and Spam Guru use multiple techniques, including multiple classifiers, to identify spam [1]. Filters for text-based spam, including plain text and HTML e-mail, have employed a variety of statistical techniques, particularly Bayesian inference; these statistical filters appear to classify text-based e-mail [2]. Spammers have recently begun developing image- based spam methods to circumvent current anti-spam technologies since existing anti-spam methods have proved quite successful at filtering text-based spam email messages. Once spammers have applied an image creation algorithm to make a message difficult to detect with computer vision algorithms, they apply further randomization to construct a batch of images for delivery. The result is that current image spam methods present serious challenges for anti-spam systems. I believe that an effective image spam detection system should satisfy several requirements. First, it should be accurate, detecting most image spam's while maintaining a low false positive rate. Second, it should be efficient, parsing incoming emails with images at modern WAN speeds. Third, it should be extensible, allowing new image spam filtering methods to be added to deal with quickly evolving image spam techniques.

3.METHODOLOGY

This proposed system is implemented from text based spam filters for detecting and blocking such spam messages [8]. Spam mails are derived as legitimate mail and illegitimate mail that is valid message and invalid message. The basic idea is used with traditional anti-spam methods to detect some image-based spam messages and fast near-duplicate detection filters to detect the variations of known spam image. The spectral clustering algorithm is used during the process of server-side filtering for identifies the real sources and large image clusters. On the client-side, principles of active learning algorithm introduced for classification accuracy and block the source address.

The Special Clustering Algorithm Steps

Given a batch of image attachments from an e-mail server, the system would first extract in variant visual features like shapes, colors, Styles to represent each image.

Dataset: Cluster of trained spam images are maintained in the server side.

Email Preprocessing: All emails are preprocessed by the preprocessor. Images are collected from emails to train the spam email detector.

Classification: These features are motivated by the fact that spam images usually present different visual statistics when compared with natural or normal images. Therefore, adopting them as visual representations may naturally discriminate spam images from normal or natural images. If the probabilities values of spam reached the threshold then the image will be send to spam of end user. Those image attachments which can pass the cluster analysis on the server side will be sent to the inbox of end users.

Image Descriptors: An image descriptor is a pair, feature vector extraction function and distance function, used for image indexation by similarity. The extracted feature vector subsumes the image properties and the distance function measures the dissimilarity between two images with respect to their properties. In these systems, image processing algorithms (usually automatic) are used to extract feature vectors that represent image properties [1] such as

1. Color Descriptor
2. Texture Descriptor
3. Local shape Descriptor

Feature Extraction

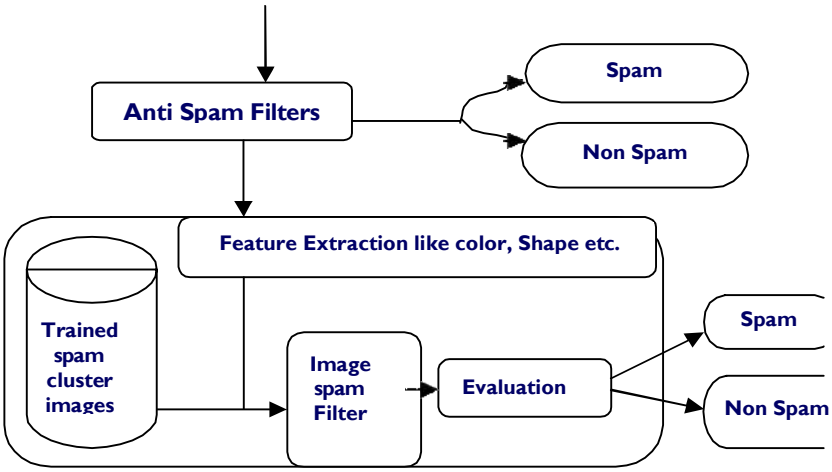
Feature extraction involves simplifying the amount of resources required to describe a large set of data accurately. When performing analysis of complex data one of the major problems stems from the number of variables involved. Analysis with a large number of variables generally requires a large amount of memory and computation power or a classification algorithm which over fits the training sample and generalizes poorly to new samples. Feature extraction is a general term for methods of constructing combinations of the variables to get around these problems while still describing the data with sufficient accuracy. These features are motivated by the fact that spam images usually present different visual statistics when compared with natural or normal images. Therefore, adopting them as visual representations may naturally discriminate spam images from normal or natural images. From this method, it can randomly pickup a set of images from data collection.

Active Learning Algorithm Steps

- Based on client side attachment, client sends the descriptor value requests and gets the spam values.
- Compare the spam values to the image attached.
- If pixel values matched then it replied notable to send the image which as identified spam.

Feature Matching

Nonnegative sparse representation introduced similarity measure to be used together with spectral clustering algorithm for clustering analysis of spam images [5]. Then relatively larger groups of images are suspected to be spam, which can be further analyzed to identify the spam sources. The spam sources can then be blocked on the server side directly without reaching e-mail users. For those spam images that survived this server-side filtering and reached the client of e-mail users, and a prototype active teaching spam hunter to enable the users to efficiently and interactively filter out the spam images. I propose a more desirable comprehensive solution which embraces both server-side filtering and client-side detection to effectively mitigate image spam. On the server side, I present a nonnegative sparsity induced similarity measure for cluster analysis of spam images to filter the attack activities of spammers and fast trace back the spam sources. On the client side, I employ the principle of active learning where the learner guides the users to label as few images as possible while maximizing the classification. The server-side filtering identifies large image clusters as suspicious spam sources and further analysis can be performed to identify the real sources and block them from the beginning.



Comparative Table

Title of paper	Authors	Approached used	Demerits	Publication
"Predicting Spam Messages Using Back Propagation Neural Network",	AK Jain, D Goel, S Agarwal, Y Singh, G.Bajaj,	Back Propagation Used for Training Neural Network for spam classification.	No preprocessing and probabilistic approach.	Springer 2020 -21, vol.110,pp.403-422.
SMSAD: A Frame work for spam Message and spam Account detection	KS Adewole, NB Anuar, A Kamsin,	Support Vector Machine Used As a classifier. Main features Are frequency of spam words and location information/phone number information.	No separate pre-processing. SVM is prone to saturation in performance	Springer vol.78, pp.78, 3925–3960.
Detecting redirection Spam using multilayer perceptron neural network	Kanchan Hans,Laxmi Ahuja, S.K. Mutto,	Scaled Conjugate Gradient (SCG) algorithm used With the aim to reduce Computational complexity For large datasets.	Doesn't Use lexical analysis.	Springer 2017. volume-1, pp.3803–3814

4. CONCLUSION

In this thesis, presented a comprehensive solution to image spam filtering, which combines cluster analysis of spam images on the server side and active learning classification on the client side for effectively filtering image spams. For server-side mitigation, I propose a nonnegative sparse representation induced similarity measure to be used together with spectral clustering algorithm for clustering analysis of spam images. Then relatively larger groups of images are suspected to be spams, which can be further analyzed to identify the spam sources. The spam sources can then be blocked on the server side directly without reaching e-mail users.

For those spam images that survived this server-side filtering and reached the client of e-mail users, proposed a prototype active learning spam hunter to enable the users to efficiently and interactively filter out the spam images. Extensive experimental evaluations of both server- side algorithms and client-side algorithms on a real image spam dataset collected from an e-mail server demonstrated the efficacy of the proposed comprehensive solution. Our future works may include, but not necessarily limited to, exploring embedded UI/UX designs to fit in our client-side active learning spam hunter with mainstream e-mail clients such as Office Outlook; investigating more discriminative image features for dealing with spam images even more effectively.

REFERENCES

1. B.Mehta, S. Nangia, M. Gupta, and W. Nejdl, "Detecting image spam using visual features and near duplicate detection," in Proc. 17th Int. World Wide Web Conf., Beijing, China, Apr. 2008.
2. M. Sahami, S. Dumais, D. Heckerman, and E.Horvitz, "A bayesian approach to filtering junk e-mail," in Proc. AAAI Workshop on Learning for Text Categorization, Madison, WI, Jul. 1998.
3. Y. Gao and A. Choudhary, "Active learning image spam hunter," in Proc. 5th Int. Symp. Visual Computing, Las Vegas, NV, Nov. 2009.
4. Jia-NingLuoMing Chuan Univ.,Taoyuan, Taiwan Ming Hour Yang, "The Bayesian algorithm for junk e- mail approach" Inf. & Telecommun.,14-16 Dec. 2009.
5. L. Benaroya, L. McDonagh, F. Bimbot, and R. Bribonval, "Non negative sparse representation for wiener based source separation with a single sensor," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Apr. 2003, vol. 6, pp. 613–616.
6. Aradhye, H. B., Myers, G. K., & Herson, J. A.(2005). "Image analysis for efficient categorization of image-based spam e-mail". Proceedings of the 2005.Eighth international Conference on Document Analysis and Recognition (ICDAR '05).
7. H. Cheng, Z. Liu, and J. Yang, "Sparsity introduced similarity measure for label propagation," in Proc. IEEE Int. Conf. Computer Vision, Kyoto, Japan, Oct. 2009.
8. Fumera, G., Pillai, I., & Roli, F. (2006). "Spam filtering based on the analysis of text information embedded into images". Journal of Machine Learning Research, 7, 2699. http://www.antiphishing.org/sponsors_technical_papers/easysol_wp_phishing_pharming.pdf
9. N. D. Lawrence, M. Seeger, and R. Herbrich, "Fast sparse Gaussian process methods: The informative vector machine," in Advances in Neural Information Processing Systems 15. Cambridge, MA: MIT Press, 2003, pp. 609–616.
10. K.-S. Goh, E. Y. Chang, and W.-C. Lai, "Multimodal concept-dependent active learning for image retrieval," in Proc. 12th Ann. ACM Int. Conf. Multimedia, New York, 2004, ACM.
11. Dave, Nakul, Uttam Chauhan, and Avani Dave. "An adaptive classification approach to filter spam e-mail using vector space model." International Journal of Management, IT and Engineering 2.8 (2012): 58-67.
12. V.Christina, S.Karpagavalli, G.Suganyca, Email Spam Filtering using Supervised Machine Learning Techniques", International journal of computer science engineering Vol.02, No.09, 2010,3126-3129.
13. Crawford, M.,Khoshgoftaar,T.M.,Prusa,I .D.etal. Survey of review spam detection using machine learning techniques. Journal of Big Data2,23(2015). https://doi.org/10.1186/s40537-015-0029-9