International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
(Vol. 09, Issue 01) and (Publishing Month: August 2014)
ISSN: 2347 - 601X
www.ijemhs.com

Analysis to Detect Pornographic Video by using Key based Search Technique

Vipin Arora[1] and Suman[2]

[1]Asst. Professor, BITS, Bhiwani, Haryana (India)
vipinarora29@gmail.com

[2]M. Tech. Student, BITS, Bhiwani, Haryana (India)
sumanjangu20@gmail.com

Abstract

In this paper here we will discuss key based search technique that is used to find out exact data stored in data warehouse in abstract fashion. Today this technique is used for detect pornography video for you tube purpose. It smallest common ancestor to identify interesting data node where sub tree contain an input set of keywords. It is a convenient and widely used approach to retrieve information from both unstructured and structured data.

Keywords: *Pornographic Video, Botnet Video, Training Data Set, Video Response Spam*

Introduction

A keyword search is sometimes called a "Boolean search" and is a commonly used method of searching for specific information in a database. This search technique allows you to retrieve all records from a database containing a particular word or a combination of words. Such a search typically generates many results that may or may not be relevant to the user's query. To obtain more useful results, techniques such as Boolean operators, truncation and nesting can be used. Keyword based search technique is applied on linguistic features to detect pornographic videos. Figure 1 shows our approach of keyword based search technique to detect pornographic video responses.

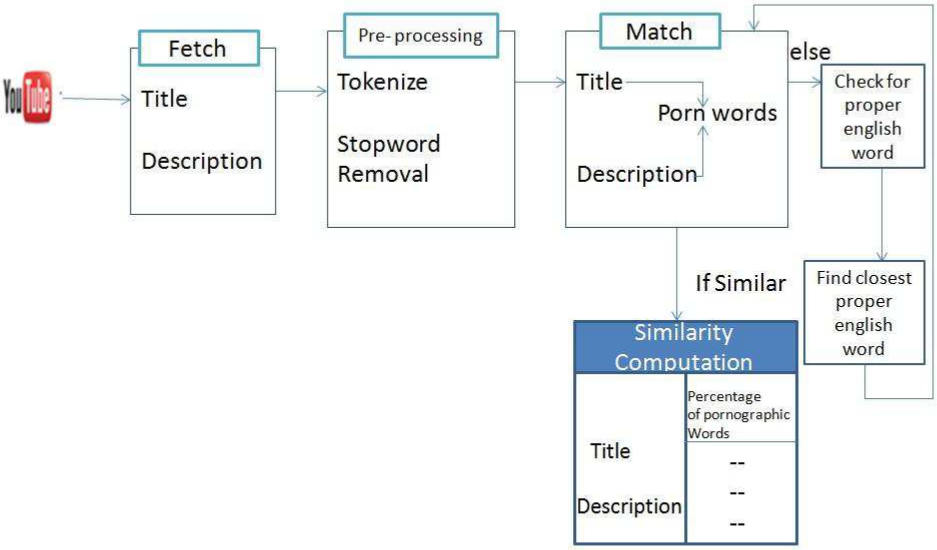


Figure 1: Keyword based search technique to detect pornographic video responses Fetch

Fetch block in figure 2 shows the retrieval of linguistic features like title and description of the YouTube video. We fetch title and description of pornographic videos through YouTube api's and apply keyword based search technique to detect presence of pornographic terms in title and description as presence of pornographic terms in title and description indicates the pornographic behavior of the video. Our hypothesis is based on the assumption that only pornographic videos contain pornographic terms in their title and description and a non- pornographic video will not contain pornographic terms.

Preprocess

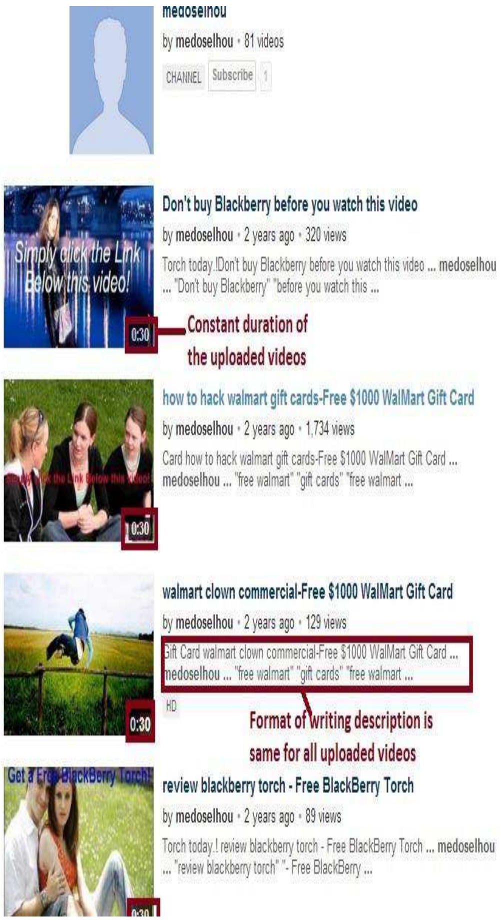
Next step is to preprocess the fetched title and description. Preprocessing involve tokenization and stop word removal. Tokenization is the process of breaking a stream of text into words called tokens. After tokenization, stop words are removed from the token list. Standard English stop word list present over the web is used to remove stop words from title and description.

Similarity Computation

In the final step, we do the matching of the tokens present in title and description with the porn words list (standard porn word dictionary present over the web) and compute the percentage of pornographic terms present in title and description. Higher the percentage of pornographic terms present in title and description, higher the chances that the video is a pornographic video.

Solution Approach to Detect Botnet Video Response

Botnet video is the video posted by an automatic script and not by a human being. Botnet video response is considered as spam because an automatic script can not analyse the content of a video and post response which is related to the main video. Figure 3 is a screenshot of a botnet profile. We notice that as botnet videos are posted by an automatic script, time.


CHANNEL
Subscribe
1
Simply click the Link Below this video!
0:30
Simply click the Link Below this video!
0:30
0:30
HD
Get a Free BlackBerry Torch!
0:30

medoselhou
by medoselhou · 81 videos

Don't buy Blackberry before you watch this video
by medoselhou · 2 years ago · 320 views
Torch today.!Don't buy Blackberry before you watch this video ... medoselhou ... "Don't buy Blackberry" "before you watch this ...

Constant duration of the uploaded videos

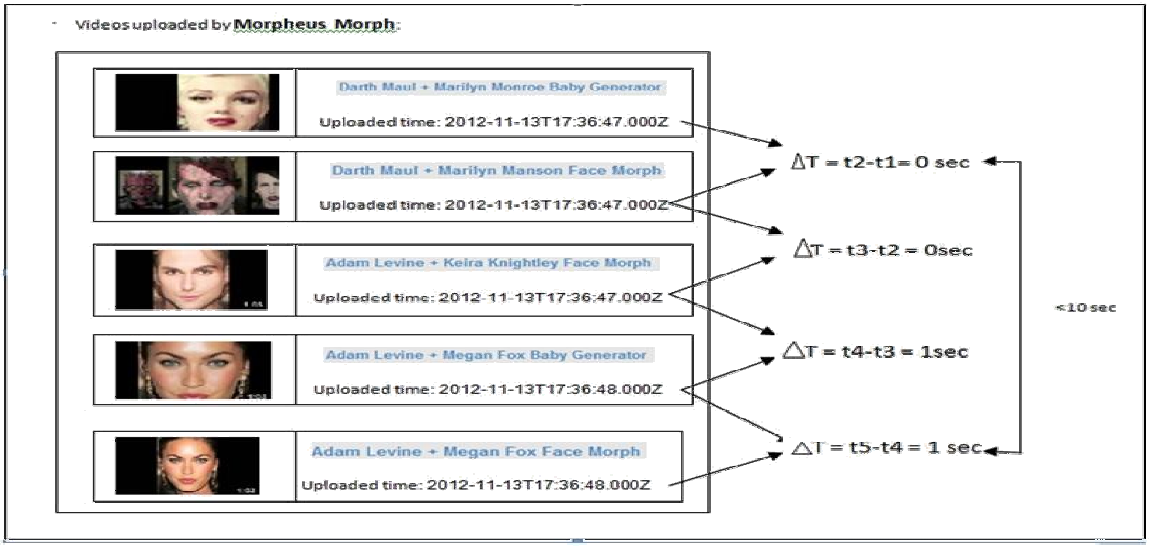
how to hack walmart gift cards-Free $1000 WalMart Gift Card
by medoselhou · 2 years ago · 1,734 views
Card how to hack walmart gift cards-Free $1000 WalMart Gift Card ... medoselhou ... "free walmart" "gift cards" "free walmart ...

walmart clown commercial-Free $1000 WalMart Gift Card
by medoselhou · 2 years ago · 129 views
Gift Card walmart clown commercial-Free $1000 WalMart Gift Card ... medoselhou ... "free walmart" "gift cards" "free walmart ...

Format of writing description is same for all uploaded videos

review blackberry torch - Free BlackBerry Torch
by medoselhou · 2 years ago · 89 views
Torch today.! review blackberry torch - Free BlackBerry Torch ... medoselhou ... "review blackberry torch" "- Free BlackBerry ...

Figure 2: Retrieval of Linguistic Features



Videos uploaded by Morpheus Morph:

Darth Maul + Marilyn Monroe Baby Generator
Uploaded time: 2012-11-13T17:36:47.000Z

Darth Maul + Marilyn Manson Face Morph
Uploaded time: 2012-11-13T17:36:47.000Z

Adam Levine + Keira Knightley Face Morph
Uploaded time: 2012-11-13T17:36:47.000Z

Adam Levine + Megan Fox Baby Generator
Uploaded time: 2012-11-13T17:36:48.000Z

Adam Levine + Megan Fox Face Morph
Uploaded time: 2012-11-13T17:36:48.000Z

Figure 3: Screenshot of a botnet profile

difference between uploaded videos is very less say few seconds. It is infeasible for a human being to upload multiple videos in very few seconds. So we fetched uploaded time of all the videos uploaded by the up loader, sort by time and compute the time difference between each successive video. if the time difference is less than a threshold, it indicates the botnet behavior of the video. Figure 4 shows our approach applied on uploaded time to detect botnet videos. Solution Approach to Detect Commercial Video Response Approach to detect commercial/promotional video response is same as pornographic video response detection. The difference is that feature set to detect commercial video is different from the pornographic video.

Classifier

In one class classification problem, either negative class is not present or it is not properly sampled. The goal of one-class classifier is to recognize spam video response. In one class classification approach, each object is represented by a vector of values, say feature vector. The algorithm does the similarity computation of new video with the existing labeled (spam) dataset to recognize video as spam i.e. pornographic, promotional, or botnet.

In this section, we describe the classifier we have developed to detect spam video responses on YouTube. The first step of the classification algorithm is to define the feature vector(set of features) which defines the feature space.

Classifier Feature Vector X is

X= (x_1, x_2,x_3 . . . ., x_n),where n = Number of features from the feature space.

n = 8 in case of Pornographic Video Response Detection,

n = 6 in case of Commercial Video Response Detection,

n = 4 in case of Botnet Video Response Detection.

The training Dataset (TD) is the set of observation vectors along with corresponding class labels. The training dataset contains data only for spam videos so class label is same for all videos presented in training dataset.

TD = ((x_1, x_2,x_4 . . . ., x_n), y_j), where j = Size of Training Dataset,

yj = Class Label.

n = 8, j = 250 in case of PVRD,

n = 6, j = 200 in case of CVRD,

n = 4, j = 61 in case of BVRD.

The testing Dataset (TS) is the vector of feature value without class label.
TS = ((x_1, x_2,x_3 . . . ., x_n)$_k$), where k = Size of Testing Dataset.

n = 8, k = 1,000 in case of PVRD,

n = 6, k = 1,000 in case of CVRD,

n = 4, k = 3,389 in case of BVRD.

Each sub-problem has multiple features; weight to each feature is assigned which shows the contribution of the corresponding feature in recognition of spam video. Let W_i = Weight of the feature i s.t.

$$\sum_{i=1}^{n} W_i = 1 \tag{3.1}$$

Input: A list L of features.

Result: Weight of each feature.

initialization;

Assign equal weight to each feature s.t

$$\sum_{i=0}^{N} W_i = 1 \tag{3.2}$$

Run the classifier and calculate the accuracy of the system, say accuracy 1.

Related Work

The work presented in this report belongs to the area of Spam detection on YouTube. In this section, we discuss some closely related work (to the experiment presented in this report) and present novel research contributions in context to existing work. We categorize the related work in 3 lines of research: Video Response Interactions and Video response spam, Social media spam detection, Classification of main aim of their work is to find evidence of pollution (opportunistic behavior of spammers and Fabricio et al. present a binary classification strategy to detect spammers on YouTube. They contrive a number of YouTube users and their profile, social behavior and finally propose a video spammer detection mechanism that classifies a user either as a spammer or a legitimate user [2]. Their results highlight the most important attributes for video response spam detection [2]. Fabricio et al. address the issue of detecting Spammers and Content Promoters and classify the real YouTube users as Spammers, Promoters or Legitimate users based on user behavior attributes. They present experimental results which demonstrate that characterization of social and content attributes is helpful to distinguish each user class [3].

YouTube videos based on contextual features.

Video Response Interactions and Video Response Spam

Fabricio et al. analyzed the properties of the social network created by video response inter-actions on YouTube [3]. They characterize users interaction with each other on YouTube to understand how malicious users can behave. The promoters). They also did some study on user behavioral patterns in video based environment [1].

Social media spam detection

Sureka present a technique to automatically detect comment spammers in YouTube Forums by mining comment activity log of a user and extracting patterns which indicates the spam behavior. Their empirical analysis on sample dataset demonstrate the effectiveness of proposed technique in identifying comment spammers [4].

Paul et al. survey potential solution for fighting spam detection on social websites like Wikipedia, Table 2.1: Literature survey of papers (chronological order) on YouTube video response spam detection using contextual features based one class classifier approach. VIVRS = YouTube video interaction and video response spam, SMS = Social media spam, CCF = classification of YouTube videos using contextual features.

Study	Type	Purpose/ Goal
Yiming et al., 1997 [7]	CCF	Presented a comparative study on Feature Selection in Text categorization
Paul et al., 2007 [6]	SMS	Survey potential solution for fighting spam on social web sites. Compare the results with prior solutions to email and web spam.
Yuan et al., 2007 [8]	CCF+SMS	Propose Contextual based analysis to automatically detect Forum spamming Define three perspective of Forum spamming and propose context- based detection technique to detect forum Spam
Fabrico et al. , 2008 [3]	VIVRS	Analyzed the properties of the social network created by video response interactions on YouTube They characterize users interaction with each other on YouTube to understand how malicious users can behave The main AIM of their work is to find evidence of pollution (opportunistic behavior of spammers and promoters) They also did some study on user behavioral patterns in Video based environment
Fabrico et al. , 2008 [4]	VIVRS	Contrive a number of YouTube users and their social behavior to discriminate a spammer from a legitimate user. Their results highlight the most important attributes for video response spam detection
Yinglian et al., 2008 [11]	SMS	Developed a spam signature generation framework for botnet spam emails detection.
Fabrico et al. , 2009 [1]	VIVRS	Instead of classifying the content of the YouTube video, they are addressing the problem of detecting spammers and content promoters on YouTube.
Benjamin et al.,2009 [12]	SMS	Study of automatic detection of spammers in a social system. Analyze distinct features that address various properties of social spam.
Fabrico et al., 2010 [2]	VIVRS	Define existing pollution in video sharing systems, their negative impact to users and systems and possible solution to minimize the problem.
Ashish Sureka, 2011 [5]	SMS	Presented a method to automatically detect comment spammers on YouTube. Technique was based on mining comments feed and extracting patterns indicating spam behavior.

Flickr and finally presented a comparative study of their work with previous e-mail and web spamming. Their paper surveys three categories of potential countermeasures which have been proposed before email and web spamming and in this paper, the author find that their applicability to social websites differs [5].

Classification of Youtube Videos Based on Contextual Features

Yiming et al. present a comparative study on feature selection methods in reduction to a high dimensional feature space in text categorization problems. Their work is motivated by the fact that as more and more information is available online, effective retrieval is difficult without good indexing. They compare 5 methods of feature selection and find the effectiveness of these feature selection methods in text categorization [6]. Yuan et al. propose context-based analysis (redirection and cloaking analysis) to detect spam automatically and to overcome shortcomings of content-based analysis. They have conducted a comprehensive study of forum spamming from three perspectives: the search user, the spammer, and the forum hosting site and showed that redirection analysis and cloaking are very effective in identifying forum spammers [7].

Research Contributions

In context to closely related work, this report makes the following novel contributions:

1. The work presented in this report is the first step in the direction of applying a one-class classifier based approach using contextual features to detect video response spam on YouTube. While there has been work done in the area of detecting video response spammers and promoters on YouTube, the application of three one-class classifiers (porno-graphic video recognition, commercial video recognition and botnet uploader detection) based on 18 video contextual features (refer to Table) offers a fresh perspective and a novel research contributions of this work.

2. We conduct empirical analysis on real world dataset acquired from YouTube to train and test the effectiveness of the proposed features and classifier. We present the intuition behind each discriminatory feature and an empirical analysis demonstrating its influence or impact on the classification task.

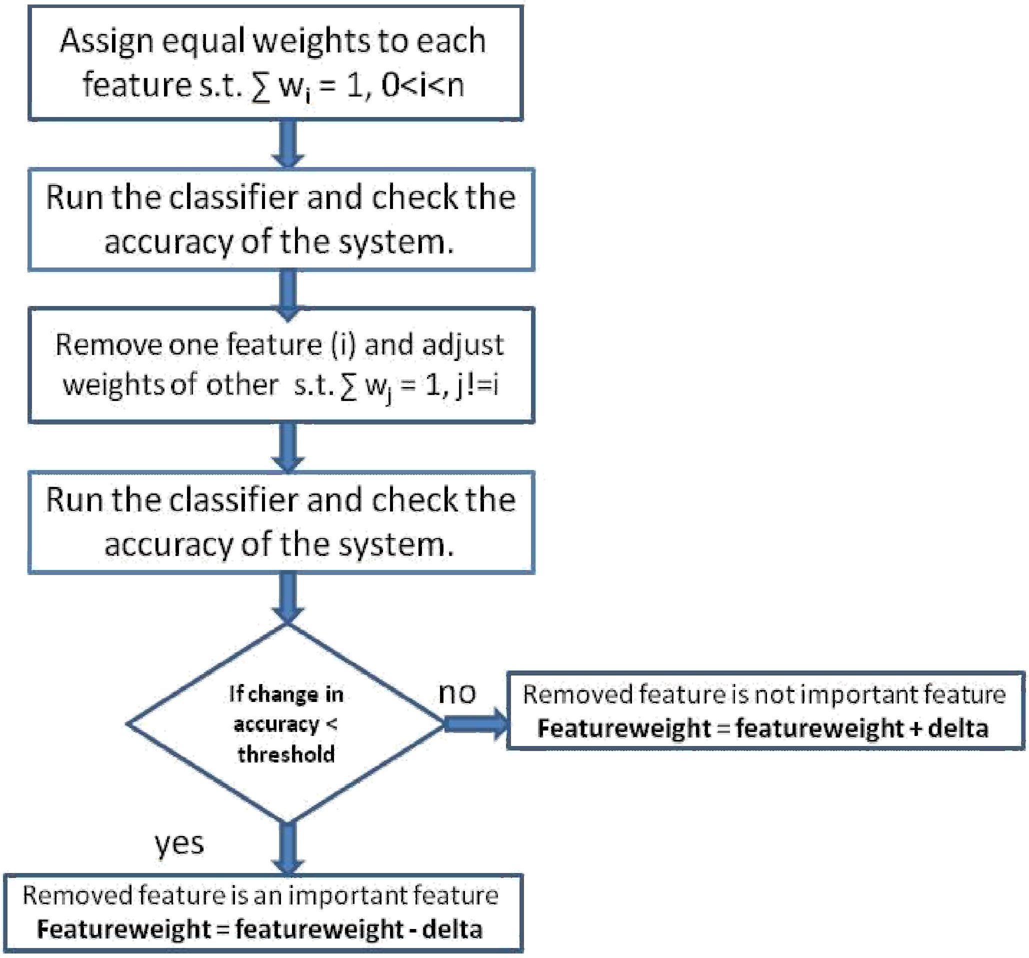

Assign equal weights to each feature s.t. ∑ w_i = 1, 0<i<n
Run the classifier and check the accuracy of the system.
Remove one feature (i) and adjust weights of other s.t. ∑ w_j = 1, j!=i
Run the classifier and check the accuracy of the system.
If change in accuracy < threshold
no
Removed feature is not important feature
Featureweight = featureweight + delta
yes
Removed feature is an important feature
Featureweight = featureweight - delta

Figure 4: Flow chart of Weight Computation

Algorithm WeightComputationEachFeature (L)

```
{
    For each feature f in L do
    {
        Remove feature j from L
        Adjust weight of rest of the feature s
        $\sum_{V=j} Wi = 1$
        Run the classifier and check the accuracy of the system, let accuracy
        Let Δ = percentage change in accuracy / 100
        If (Significant change in accuracy) then
            Removed feature is an important feature weight correspondingly
            To this feature should be high
            $\text{Feature}_{\text{Wt I =}}\text{Feature}_{\text{Wt i}}$
        Else
            Removed feature is not an important feature and weight corresponding to this feature should be low
                $\text{Feature}_{\text{wt I}} = \text{Feature}_{\text{Wt I + 1}}$
            }
```

Algorithm 1 shows our approach of calculating the weight of each feature where the whole process is repeated until the accuracy is optimal. The result of the algorithm shows the contribution of each feature in the spam video response detection. Lower the weight, more important the feature is. Figure 5 shows the fow chart of computing weight of each individual feature based on their influence.

One class classification **approach** is based on similarity computation; we need to find the similarity of the new object with the existing dataset which is the score of that particular feature. Score of the feature is a unique value which represents that feature in comparison to the training dataset.

S_i = Score of the feature i s.t.

$0 \leq Si \leq 1$

Our experimental dataset consists of both numerical features (nf) like duration of the video, number of subscribers etc and categorical features (cf) like category of the YouTube video; there are different approaches to calculate score of these features. For numerical features, we are calculating the average difference of the new object with the existing training dataset. Lower the difference, higher the chance that new object is similar to the existing dataset. For categorical features, percentage of videos fall into the specific category contributes in finding the score of the feature.

If j is the size of training dataset, then equation to score of numerical feature is:

$$\boxed{c_{value} = \sum_{i=0}^{n} W_i * S_i}$$

$$\boxed{Score_{nf} = \sum_{i=0}^{j} (|(new_{value} - TS[i])|/n)}$$

This equation of calculating score of numerical feature is not applicable to all the numerical features because for certain features like percentage of pornographic terms in title and description, higher the number of dirty terms present, higher the chances that video is a pornographic video. For such features, let x = Percentage of pornographic or commercial terms present in title or description.

$\boxed{Score_{nf} = 1-(x=100)}$

Let y = Percentage of videos fall in the particular category

$\boxed{Score_{cf} = 1-(y=100)}$

Because we consider the average difference, lower the value of the score, higher the chance that new object is similar to the training dataset objects. Based on weight and score of each feature, we compute the final value of the feature, C_{value} which is the resemblance of the feature with the target class and recognizes the Spam behavior of the video.

References

[1] Benevenuto, Fabricio, Fernando Duarte, Tiago Rodrigues, Virgilio AF Almeida, Jussara M. Almeida, and Keith W. Ross. \Understanding video interactions in YouTube." In Proceedings of the 16th ACM international conference on Multimedia, pp. 761-764. ACM, 2008.

[2] Benevenuto, Fabricio, Tiago Rodrigues, Virgilio Almeida, Jussara Almeida, Chao Zhang, and Keith Ross. \Identifying video spammers in online social networks." In Proceedings of the 4th international workshop on Adversarial information retrieval on the web, pp. 45-52. ACM, 2008.

[3] Benevenuto, Fabricio, Tiago Rodrigues, Virgilio Almeida, Jussara Almeida, and Marcos Goncalves. \Detecting spammers and content promoters in online video social networks." Proceedings of the 32nd international ACM SIGIR conference on Research and development in information retrieval. ACM, 2009.

[4] Sureka, Ashish. \Mining user comment activity for detecting forum spammers in YouTube." Inter-national workshop on USEWOD co-located with WWW2011.

[5] Heymann, Paul, Georgia Koutrika, and Hector Garcia-Molina. \Fighting spam on social web sites: A survey of approaches and future challenges." Internet Computing, IEEE 11.6 (2007): 36-45.

[6] Yang, Yiming, and Jan O. Pedersen. \A comparative study on feature selection in text categoriza-tion." MACHINE LEARNING-INTERNATIONAL WORKSHOP THEN CONFERENCE-. MOR-GAN KAUFMANN PUBLISHERS, INC., 1997.

[7] Niu, Yuan, Yi-Min Wang, Hao Chen, Ming Ma, and Francis Hsu. \A quantitative study of forum spamming using context-based analysis." Proc. of 14th NDSS (2007).