ReP-ETD: A Repetitive Preprocessing Technique for Embedded Text Detection from Images in Spam Emails

Asha S Manek
Assistant Professor

Shirdi Sai Engineering College, Bangalore
Department of Computer Science and Engineering
Research Scholar,
Jawaharlal Nehru Technological University
Hyderabad, India
ashas100@gmail.com

M. Chandra Mohan
Department of Computer Science and Engineering
Jawaharlal Nehru Technological University
Hyderabad, India

Shamini D K
UVCE
Bangalore University
Bangalore, India

Venugopal K R
University Visvesvaraya College of Engineering
Bangalore University
Bangalore, India

Veena H Bhat
IBS Bangalore
Bangalore,
India

P Deepa Shenoy
Department of CSE
University Visvesvaraya College of
Engineering
Bangalore University
Bangalore, India

L M Patnaik
Honorary Professor
IISC
Bangalore, India

Abstract—Email service proves to be a convenient and powerful communication tool. As internet continues to grow, the type of information available to user has shifted from text only to multimedia enriched. Embedded text in multimedia content is one of the prevalent means for delivering messages to content viewers. With the increasing importance of emails and the incursions of internet marketers, spam has become a major problem and has given rise to unwanted mails. Spammers are continuously adopting new techniques to evade detection. Image spam is one such technique where in embedded text within images carries the main information of the spam message instead of text based spam. Currently, image spam is evaluated to be roughly 50% of all spam traffic and is still on the rise, thus a serious research issue. Filtering mails is one of the popular approaches used to block spam mails. This work proposes new model ReP-ETD (Repetitive Pre-processing technique for Embedded Text Detection) for efficiently and accurately detecting spam in email images. The performance of the proposed ReP-ETD model has been evaluated across the identified parameters and compared with other existing models. The simulation results demonstrate the effectiveness of the proposed model.

Keywords—Spam Detection, Preprocessing Techniques, ReP-ETD, Image Spam.

I. INTRODUCTION

Nowadays, email service is one of the convenient communication applications on the web and is an integral part of our life. While enjoying the facilities of email service, users are also facing the problem of email spam. Email spam is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email also known as junk email or Unsolicited Bulk Email (UBE). Spam is depicted as ubiquitous and unavoidable. The increase in the volume of spam emails has decreased the quality of email service and has lead to the increase in the cost of storage resources as well as communication bandwidth. Moreover, news¹ reports that spam produces millions of tons of CO₂ globally every year. Carbon Footprint of email spam report estimates that 62 trillion spam emails are sent globally every year. Searching for legitimate emails and deleting spam uses around 80% of

energy. The study found that the average business user generates 131kg of CO₂ every year, of which 22% is related to spam.

For effective spamming, spammers are adapting new and innovative techniques like email appending, image spam, blank image and backscatter spam.

Email Appending: If a marketer has one database containing names, addresses, and telephone numbers of prospective customers, they can pay to have their database matched against an external database containing email addresses. The company then has the means to send emails to people who have not requested emails, which may include people who have deliberately withheld their email address for the sake of privacy[1].

Image Spam: Image-based spam[2][3] is an obfuscating method in which the text of the message is stored as a GIF or JPEG image and displayed in the email. This prevents text based spam filters from detecting and blocking spam messages.

Blank Image: Often in emails, the message body as well as the subject line will be missing intentionally. Still, it fits the definition of spam as it is bulk and unsolicited email. Blank spam originates in different ways, either intentionally or unintentionally:

- 1) Blank spam can be sent in a directory harvest attack, a form of dictionary attack for gathering valid addresses from an email service provider.
- 2) Blank spam may also occur when a spammer forgets or otherwise fails to add the payload when he or she sets up the spam run.
- 3) Often blank spam headers appear truncated, suggesting that computer glitches may have contributed to this problem from poorly written spam software to malfunctioning relay servers, or any problems that may truncate header lines from the message body.
- 4) Some spam may appear to be blank when in fact it is not. An example of this is the VBS.Davinia.B email worm [4] which propagates through messages that have no subject line and appears blank, when in fact it uses HTML code to download other files.

¹ See <http://news.bbc.co.uk/2/hi/technology/8001749.stm>

Backscatter Spam: Backscatter is a side-effect of email spam, viruses and worms, where email servers receiving spam and other mail send bounce messages to an innocent party. This occurs because the original message's envelope sender is forged to contain the email address of the victim.

According to IBM X-Force 2012 Mid-year Trend and Risk Report, at the end of 2011 is the rebirth of image based spam. Spammers continued to use this type of spam until the end of March 2012. At one time, more than 8% of all spam contained an image attachment.

Many solutions are proposed for detecting and filtering spam emails. To get rid of anti-spam filters in email spam currently some spammers put their spam content into the images (i.e. they embed text such as advertisement text in the images) and attach these images to emails. Those anti-spam filters that analyze content of email cannot detect spam text in images.

Following characteristics are noticed in the image spam data set collected for this work:

- *Repetitiousness:* The identical content sent by spammers many times to the same email account.
- *Variability:* Spammers usually produce many variations for a template image spam to circumvent simple signature-based anti-spam filters. The tricks of making image variations include translation, rotation, scaling, local changes and adding random noises etc.
- *Commonness:* Most of image spams contain embedded text.

Based on the above observations, ReP-ETD a new model is proposed in this work to improve accuracy using repetitive preprocessing in detecting image spams containing embedded text from large corpus.

In this paper, a brief description of the background work given in section II. Section III discusses about related work, Section IV problem statement, Section V Motivation and Section VI outlines the details regarding implementation of the proposed model ReP-ETD, the data set details, and the pre-processing framework. Results and performance analysis are discussed in section VII. Conclusion and future works are presented in section VIII.

II. BACKGROUND WORK

Spam is not just limited to email anymore, it is on VoIP in the form of unsolicited marketing or advertising phone calls, or marketing, advertising and pornography links on social network. Spam is everywhere!

There are many ways spammers can get to know your email address and send you spam even though you may never open any spam mails or click any suspicious links. If you are on any social network and do not set your privacy settings correctly, your data is available to anyone who includes your location, email and friend lists etc. Dictionary attack is one of the techniques to harvest email addresses. So it is easy to find information with little time and effort and spammer have lots and lots of it. Most of the spammers use bots to do the job for them so even if they get one user

to respond to their spam it is worth the effort to send email to hundreds of people. Filters today can arrest most of the email spam that appears in the form of text.

Image spam is a variant of email spam where the spammers actually embed the spam message in an image instead of directly placing it as mail content to evade spam filters. Spam filters look for certain key words like Viagra, cash, money which are commonly related to spam emails. However when message is inside an image the spam filters cannot effectively filter these messages. There are many techniques which spammers used to obfuscate spam filters. Some examples are[5]

- Adding random words before HTML
- Use white text on white background
- Using characters like C*ash
- Adding bogus HTML tags with lot of text
- Adding spaces in words like "M o n e y "

As stronger filters were developed to track these messages, spammers came up with newer techniques like image spam, using PDF documents to send spam etc. With the use of Optical Character Recognition (OCR) filters it is possible to extract the contents of the images and then check if the image had spam content. However, spammers have come up with new ways to evade the OCR filter. Some of the ways include

- By rotating images or making them look wavy
- Adding noise to the images
- Slice the image and rotate each component.

Hence, ReP-ETD, a unique model proposed for the detection of image spam using repetitive preprocessing technique for embedded text in spam emails considering only text features which is very cost effective.

III. RELATED WORK

Image spam has not been studied as extensively as email spam; however some recent research works have explored image spam involving detection of text in the spam message, or identifying low-level features like header properties and histogram. Artificial Neural Networks (ANN) has been used for identifying image spam. The images are first normalized into grayscale values between 0-1. Then an ANN was trained on these images using a supervised learning approach and the model was tested for classification of new samples of spam images. The classification accuracy of about 70% was reported for unseen images[6].

Low-level features like image width, height, aspect ratio, file size, compression and image area are all extracted from the image header and have been used along with another set of features like the number of colors and variance, frequently occurring colors and primary color in image and then color saturation and color histograms were also computed. A set of binary features was used to indicate file type (JPEG or BMP or PNG). SVM classifiers were used to classify images. Accuracy over 95% was

reported[7].

Aradhaye et al., used their existing work to detect text embedded in digital photographs. The text was analyzed on extraction and features like color saturation, color heterogeneity feature were computed. SVM classifier was used to classify images. An accuracy of 85% [8] was achieved.

Similar features as in [7] were used in another study for classification using C4.5 decision tree and SVM algorithm in Weka. Their results indicated that support vector algorithms performed better than C4.5 as it had a larger area under the ROC curve [9].

A prototype system to detect the spam images in email is discussed in [10]. A probabilistic boosting tree based on the training set to distinguish spam images from ham images was built and the model demonstrated an accuracy of about 89%.

Yan Gao et al [11] proposed a semi-supervised system prototype based on a regularized discriminant Expectation Maximization algorithm to detect the spam images attached in emails. The proposed method employs a small amount of labeled data and extracts efficient image features to perform both transductive and inductive learning to detect the spam image and achieves results of 88.40% of true positive rate.

Giorgio Fumera, Ignazio Pillai and Fabio Roli [12] proposed an approach to antispam filtering which exploits the text information embedded into images sent as attachments. Their approach is based on the application of state-of-the-art text categorization techniques to the analysis of text extracted by OCR tools from images attached to emails.

Mark Dredze, Reuven Gevartyahu and Ari Elias-Bachrach [13] introduced Just in Time (JIT) feature extraction, which creates features at classification time as needed by the classifier. They demonstrated JIT extraction using a JIT decision tree that further increases system speed. Image spam classification provides accuracy of 99% and a method to learn fast classifiers.

IV. PROBLEM STATEMENT

Given a set of image data as mentioned in table I, the aim of this research work is to detect the spam in the email images. To identify the spam content in the images, the following assumptions are made

- Blank images which do not have either text or image content do not serve the purpose of proposed model ReP-ETD as our intention of classification is mainly content oriented.
- Image spam is the conveyor of mainly textual spam message in a different format to fool the anti spam filters. Hence, proposed model ReP-ETD based on the textual content in the images.
- Working on large dataset can show the robustness of the proposed model.

V. MOTIVATION

In web and email applications, the number of images with embedded text has increased rapidly. Being able to detect text embedded in these images will be a good starting point to further analyze the received contents. One example is the Unsolicited Commercial Email (UCE), also known as "spam", on the Internet. With the increasing importance of email and the incursions of internet marketers, spam has become a major problem. Image spam is a variant of email spam where the spammers actually embed the spam message in an image instead of directly placing it as mail content to evade spam filters. Recently, spammers have been using embedded-text in images to avoid the text-based anti-spam filters. Without the ability to detect embedded-text, it will be very difficult to alleviate this problem. This forms the first motivation to our work. The second motivation for our work is to improve accuracy in detecting spam in the embedded text in images using repetitive preprocessing on large data set.

VI. IMPLEMENTATION

A. Data Source

To identify image spam mails, the data set used in this work are imageSpamDredze, imageSpamISH, imageSpamTrec07 and personal image corpus. The total numbers of spam images are 8274 and ham images are 3676, thus a total of 11950 mails embed the spam message in an image.

TABLE I LIST OF DATA SET USED FOR MODEL ReP-ETD

Data set	Ham Images	Spam Images
ISH	784	896
Dredze	1000	3171
Trec07	1227	869
Personal Image	665	3338

B. Modeling

1) The main step in the ReP-ETD includes a focused preprocessing stage, followed by classification and performance analysis. Figure 1 illustrates the architecture of the proposed model.

Pre-Processing: Figure 2 illustrates the pre-processing model proposed by this research work. The identified data set consisting of both ham and spam image emails are pre-processed to identify the bag-of-words from the intermediate data set and it is a user interactive process.

The steps involved in the initial analysis of images:

- Step 1: Removal of corrupted images from the data set that is considered for analysis.
- Step 2: Removal of images which is not recognized as valid image format by our OCR tool.
- Step 3: Conversion of all images into grayscale to reduce the noise overhead that is introduced by the CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)

technique used by the spammers.

- Step 4: The OCR tool used in our work is ABBYY Fine Reader 9.0 Sprint with default settings to retrieve the images in the Portable Document Format (PDF) for further processing in RapidMiner. Using this technique, we ensured manually that there is no loss of data by our OCR technique.
- Step 5: The text extracted from the images undergoes various sub-stages which includes transforming text into lower cases to reduce the case sensitiveness, stop words removal, filtering of less weighted words, etc.
- Step 6: The crucial stage is to select the ‘bag of keywords’ which successfully distinguishes between spam and ham.
- Step 7: Selection of keywords is done by applying Bayes theorem for calculating the probability of occurrence of “to be called spam words“ from the extracted text embedded in the images.

Fig 1: Architecture of ReP-ETD model

The implementation of Bayes theorem is

$$p(\text{word/spam}) = \{p(\text{word/spam}) * p(\text{spam})\} / p(\text{word}) \quad \text{---(1)}$$

where

$p(\text{word/spam})$ -> probability of occurrence of word in spam images.

$p(\text{spam})$ -> probability of total spam images in the data set.

$p(\text{word})$ -> probability of the word in the whole data set.

Fig 2: Process in the Pre-processing Stages in reading PDF files

- Step 8: The occurrence of one of the keywords from the bag of keywords and the number of times it occurs is taken into consideration to determine the nature of input image (as spam /ham).

Unique feature of ReP-ETD model is that few keywords are selected when compared to other works and is undergone repeated pre-processing for improving results as shown in fig 2. Hence the data mining solution becomes simpler and faster. The Table II list the 10 identified keywords that form our ‘bag of spam keywords’ is selected based on their occurrences in data set.

Once the bag-of-words is created, the next process involves the generation of the data set that captures the pattern for ham and spam images used as the input to the training model. Every image file i.e PDF file considered is represented as an instance in the data set which has a value between ‘1’ and ‘0’ representing the weighted presence of the word.

This pattern is generated for all the images of data set chosen. There could be a few emails which has images with embedded text in which, none of the selected keywords might be present. Such text embedded images are identified and are pre-processed again instead of misclassifying them in order to reduce the error rate. Thus accuracy can be increased.

TABLE II LIST OF FEW OF THE KEYWORDS & FREQUENCY OF OCCURRENCES

Keywords	Frequency	Keywords	Frequency
Viagra	5204	browser	2406
click	4267	xanax	2153
ciali	4216	pill	2072
price	3797	address	2057
type	2471	ambien	1931

2) *Classification*: The preprocessed data is trained and evaluated using W-Random Tree and W-Random Forest classifiers. The model is cross validated using split validation operator with split ratio between 0.5-0.9. The simulated results were evaluated after running the test phase.

VII. RESULTS AND PERFORMANCE ANALYSIS

A. Supervised Learning Results

Rapid Miner (YALE Yet Another Learning Environment) is an open source statistical and data mining package written in Java is used to implement our model. It is a simple, efficient tool that supports image processing, data loading, transforming and flexibility to implement a customized data pre-processing, modeling and evaluation of the implemented model.

Accuracy of a classifier is an important criteria where in it decides whether training model has or not correctly predicted the actual classification in the test data.

The following table III shows a confusion matrix which depicts how predictions on instances are tabulated:

TABLE III CONFUSION MATRIX

		Actual Class (Observation)	
		True Ham	True Spam
Predicted Class (Expectation)	Pred. Ham	TP (Correct Result)	FP (UnexpectedResult)
	Pred. Spam	FN (Missing Result)	TN (Correct absence of Result)

A confusion matrix can be summarized using various formulas:

Accuracy: The percentage of predictions those are correct.

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN}) \quad (2)$$

Precision: The percentage of positive predictions those are correct.

$$\text{Precision} = \text{TP} / (\text{TP} + \text{FP}) \quad (3)$$

Recall: The percentage of positive labeled instances that were predicted as positive.

$$\text{Recall} = \text{TP} / (\text{TP} + \text{FN}) \quad (4)$$

The proposed model works efficiently for large data sets and takes only still images as input.

TABLE IV RESULTS OF THE PROPOSED MODEL MODEL FOR TREC07+DREDZE+ISH+PERSONAL DATA SET

Classifier	Accuracy %	Precision %	Recall %
W-Random Forest	99.83	100	99.83
W-Random Tree	99.83	100	99.83

The output of the proposed pre-processing model was given as input to the following identified classifiers individually, W-Random Forest, W-Random Tree, W-IBk, W-BIF Reader, K-NN, SVM, Naïve Bayes and SVM-linear.

The performance parameters accuracy, recall and precision were calculated and the values are tabulated in table IV combining all four data set with spilt ratio of 0.9 and linear sampling. Table V shows results of the proposed model of ISH and Dredze corpus.

TABLE V RESULTS OF THE PROPOSED MODEL OF ISH AND DREDZE COPRUS

Classifier	Accuracy %	Precision %	Recall %
W-Random Forest	99.81	100	99.81
K-NN	88.38	99.12	83.83
W-Random Tree	99.81	100	99.81
W-IBk	88.38	99.12	83.83
Naives-Bayes	87.86	99.40	82.84
SVM-linear	68.03	100	53.48

B. Performance Evaluation

Random forests work by generating (typically hundreds) of decision trees in a specific random way such that each is de-correlated with the others. Since each decision tree is a low-bias, high-variance estimator, and each is relatively uncorrelated with the others, when we aggregate their predictions we get a final prediction with low bias and low variance. The reason behind choosing w-random forest algorithm are-it is robust to different variable input types, missing data, and outliers; it has been shown to perform extremely well across large classes of data and

scales reasonably well computationally.

The proposed architecture ReP-ETD, gives far better performance, when evaluated with identical experimental settings as described in the compared works. For the purpose of the comparative study with the work[14][15], we have evaluated the results by combining all data set. The keywords obtained from individual corpus are found to be present in combined approach of our model.

i) Comparison of ReP-ETD with work[14]

Congfu Xu et al., in their work[14], have presented a novel hybrid framework for detecting spam email with content embedded in images by fusion of the classifiers. Given a spammed image, their method has been able to extract both the text and image features and input the vector into the bottom-layer classifiers respectively and obtains the final decision based on the fusion of the outputs of the classifiers. Using seven keywords feature space and the corpora are collections of personal emails used containing 2006 ham images and 3297 spam images. Results published prove that the fusion classifier with an SVM combines the classification performance from the text and image classifiers in a complementary fashion.

The response of ReP-ETD, when used with W-Random Tree and W-Random Forest classifiers on the 10-attribute input showed us that ReP-ETD is more sensitive and accurate in spam detection when considered only text features than the hybrid framework proposed in work[14]. Table VI illustrates the same.

TABLE VI COMPARISON OF PERFORMANCE OF ReP-ETD WITH CONGFU XU ET AL[14]

Feature Space	CONGFU XU ET AL[14]	Our approach
Data set used	Spamassasin	Trec07+Dredze+ISH +Personal
Classifier	SVM	W-Random Tree, W-Random Forest
Features	text & image	only text
Accuracy	98.205%	99.83%
Recall	Below 40%	99.83%
Precision	100%	100%

ii) Comparison of ReP-ETD with work[15]

Basheer al-Duwairi et al[15] proposed technique called Image Texture Analysis-Based Spam Filtering (ITA-ISF), extracts features related to the histogram, gradient, run-length matrix, co-occurrence matrix, autoregressive model, and wavelet transform of an image and applies a feature selection algorithm to reduce the feature space while keeping the most informative features. The performance of C4.5 Decision Tree(DT), Support Vector Machine (SVM), Multilayer Perception (MP), Naïve Bays (NB), Bayesian Network (BN), and Random Forest (RF) machine learning classifiers were applied on the low-level image texture features of two publicly available data sets (3209 spam, 1770 ham from Dredze et al. 926 spam, 810 ham from Image Spam Hunter (ISH).

TABLE VII COMPARISON OF PERFORMANCE OF ReP-ETD WITH BASHEER AL-DUWAIRI ET AL[15]

Proposal	BASHEER AL-DUWAIRI ET AL[15]	Our approach	Our approach
Data set used	Dredze and ISH	Trec07+Dredze +ISH+Personal	Dredze and ISH
Classifiers	DT,SVM,MP, NB,BN,RF	W-RT,W-RF	W-RT,W-RF
Features	Image & Text	Only text	Only text
Accuracy	98.1%	99.83%	99.81
Recall	98.1%	99.83%	99.81
Precision	98.6%	100%	100

Performance evaluation of the proposed model compared to image spam filter[15] shows that the W-Random Tree and W-Random Forest classifier outperforms all the other classifiers with an average precision, recall and accuracy of 99.83%. For efficient comparison with[15] considering only Dredze and ISH data set, the proposed model shows 99.81% accuracy and precision as in the Table VII.

The data mining solution in[14][15] proposes mainly image feature manipulation which requires more of cost and time investment. Hence, ReP-ETD proposes the detection of image spam in a cost effective way considering only text features because the main intention of spammers is Sales, Promotion And Marketing and practically, about only 2% of our inbox is clogged with image spam per week.

VIII. CONCLUSION AND FUTURE WORK

In this work an approach to anti-spam filtering which exploits the text information embedded into images sent as email attachments is proposed. This approach extracts embedded text from attached images. The effectiveness of this approach has been evaluated on three large data sets of publicly available Trec07, Dredze, ISH and personal corpus of emails contained attached images. Experiments show that, the proposed approach allows the improvement of the categorization accuracy of 99.83% on emails which contained text embedded into attached images. The proposed model works efficiently for large data sets.

The main limits of these experiments are - Firstly, very few legitimate emails contained text embedded images in our experiments (although legitimate emails in which the whole text message is embedded into an image are likely to be much rarer than spam emails). Secondly, the proposed model works on still images only. An OCR software used is not optimized for this task, neither from the viewpoint of the specific kind of images to be processed, nor from the viewpoint of the computational complexity. Nevertheless, we believe that our results are a first clear indication that exploiting text information embedded into images attached to spam emails using repetitive pre-processing technique, as in the proposed approach, can effectively improve the categorization accuracy of server-side spam filters. These results are relevant given that an increasing fraction of

spam emails has text embedded into images, although it is likely that in the future spammers will also apply content obscuring techniques to images, to make OCR systems ineffective without compromising human readability.

Accordingly, applying repetitive pre-processing on large image data set to analyse the robustness of the approach proposed in this paper is an interesting development of our work.

References

- [1] Bob West, "Getting it Wrong: Corporate America Spams the Afterlife", Clueless Mailers. (January 19, 2008) Retrieved 2010-09-23.
- [2] Fumera, Giorgio, Ignazio Pillai, and Fabio Roli. "Spam filtering based on the analysis of text information embedded into images", The Journal of Machine Learning Research vol.7, pp. 2699-2720, 12/2006.
- [3] Battista Biggio, Giorgio Fumera, Ignazio Pillai, Fabio Roli, "A survey and experimental evaluation of image spam filtering techniques, Pattern Recognition Letters". Volume 32, Issue 10, pp 1436-1446, ISSN 0167-8655, 15 July 2011.
- [4] Symantec.com, "symantec.com", Retrieved 2012-12-10.
- [5] Spammer's Compendium, <http://www.jgc.org/tsc.html>, last accessed date 03/24/2010.
- [6] Hope, P., Bowling, J. R., and Liszka, K. J., "Artificial Neural Networks as a Tool for Identifying Image Spam", The 2009 International Conference on Security and Management (SAM'09), pp. 447-451, July 2009.
- [7] Chao Wang, Fengli Zhang, Fagen Li, Qiao Liu, "Image spam classification based on low-level image features", Communications, Circuits and Systems (ICCCAS), 2010 International Conference on, pp.290-293, 28-30 July 2010.
- [8] Aradhye, Hrishikesh B., Gregory K. Myers, and James A. Herson, "Image analysis for efficient categorization of image-based spam e-mail." In Document Analysis and Recognition, 2005. Proceedings. Eighth International Conference on, IEEE pp. 914-918, August 2005.
- [9] Krasser, S.; Yuchun Tang; Gould, J.; Alperovitch, D.; Judge, P.; , "Identifying Image Spam based on Header and File Properties using C4.5 Decision Trees and Support Vector Machine Learning," Information Assurance and Security Workshop, 2007. IAW '07. IEEE SMC , vol., no., pp.255-261, 20-22 June 2007.
- [10] Yan Gao, Ming Yang, Xiaonan Zhao, Bryan Pardo, Ying Wu, Thrasivoulos N. Pappas, Alok Choudhary, "Image Spam Hunter", EECS Dept., Northwestern Univ., Evanston, IL, Proceedings Acoustics, Speech and Signal Processing, 2008. ICASSP 2008.
- [11] Yan Gao, Ming Yang, and Alok Choudhary, "Semi Supervised Image Spam Hunter: A Regularized Discriminant EM Approach", In Advanced Data Mining and Applications, pp. 152-164. Springer Berlin Heidelberg, 2009.
- [12] Giorgio Fumera, Ignazio Pillai and Fabio Roli, "Spam Filtering Based On The Analysis Of Text Information Embedded Into Images", Journal of Machine Learning Research 7 (2006) 2699-2720, Submitted 3/06; Revised 9/06; Published 12/06.
- [13] Mark Dredze, Reuven Gevartyahu and Ari Elias-Bachrach, "Learning Fast Classifiers for Image Spam", CEAS. 2007.
- [14] Congfu Xu, Kevin Chiew, Yafang Chen and Juxin Liu, "Fusion of Text and Image Features: A New Approach to Image Spam Filtering", Y.Wang and T. Li (Eds.): Practical Applications of Intelligent Systems, AISC 124, pp. 129-140. springerlink.com Springer-Verlag Berlin Heidelberg 2011.
- [15] Basheer Al-Duwairi, Ismail Khater and Omar Al-Jarrah, "Detecting Image Spam Using Image Texture Features", International Journal for Information Security Research (IJISR), Volume 2, Issues 3/4, pp 344-353, September/December 2012.