International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 2, No. 1, 2015, pp. 51-58.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

A Method for Image Spam Detection Using Texture Features

Monireh sadat Hosseini[a] , Mohammad Rahmati[b]

[a] *MSc Student, Islamic Azad UniversityofBouin Zahra, Department of Computer Engineering, Faculty of Engineering, BuinZahra, Iran.*

[b] *Associate Professor, Department of Computer Engineering and Information Technology,Amirkabir University of Technology(Tehran Polytechnic).*

Abstract

By increasing of e-mail, the received junk mail has become a challenge, which is called spam e-mails. To detect image spam, computer vision techniques can be used. In this article, a method to increase of the accuracy of identification and classification of spam or non-spam valid images is personated. In this method, image texture features are used to evaluate the image. In this study, the gray level co-occurrence matrix (GLCM) is used that is one of the characteristics of the texture. After extraction matrixes from images , for each image, was obtained 22 features. Then the k-nearest neighbor classifier (KNN) and naive Bayesian (NB) are used to classify images with features that obtained of each images. The images obtained from the both of works database Dredze and ISH. In this method, presented results were given with compare the last works indicative of importance classification in accuracy.

Keywords: Spam images, Image texture, GLCM, Classification

Introduction:

Send e-mail is universal activity in the transmission field of messages on internet. By increasing use of this approach, some of people and companies start to sending e-mail to various reasons in commercial, political, religious, with different content for users of these service. It is called spam or junk, that was sent as officious for users[1]. This phenomenon has been seriously challenged by email, and accordingly checking with spam is considered as a major subject of research. According to reports, more than half of the emails are sent every day are spam and high volume of internet lines is wasted as well as great cost to manage spam to users is imposed, which causes loss of memory and network recourse such as network congestion . Create a spam filters is one of the main ways to deal with spam ,that these methods are based on techniques of computer vision and pattern recognition. Spammers or spam Creators, in order to avoid detection by these filters, invented a new method that content of spam messages sent in the form of wallpaper that This type of e-mail , Said image spam . This technique was started in 2005 and grew rapidly. For example, an advertisement text within an image can be placed. So that it becomes impossible to analyze the content of messages with simple filters. So you need to filter that can correctly detect spam images. The main function of this type of filters, to find a high-performance algorithms to identify spam images from non-spam images[2]. In this paper, using the gray level co-occurrence matrix (GLCM) of the image texture features to detect image spam and then classify this type of images.

Problem Statement and previous work

2.1 image spam

Manufacturer spam to pass filters created based on text filtering, used the images because it is much more difficult to detect than text. A few examples of image spam are shown in Figure 1. The researchers noted different definitions of spam images that we give a few of them:

Image spam is said to have an image advertisement that message included in the original image or attached to the main body[3]. Image spam is a spam e-mail or text message spam is shown as a picture file. That's mean The image as a graphics mode and text-based email, or images that contain links and URL links are directed to web pages anonymously. There are different definitions of this type of email.[4] In general, techniques to detect spam images are divided into 3 categories.

- Header based techniques eliciting the spam email properties for analyzing and detection

Header is always the content of the message to the user. It is specific to review the e-mail header. Which contains a lot of useful information to provide .

in saraubon and limithanmaphon [5] have presented a spam filter that works by e-mail header. The authors make to these filters both spam based on text and image, as well as identify. They only use the IP address of the sender and the sender's email address by its IP address belongs to detect. In Krasser et al, [6] only length and width of the header file, image file types and sizes have used it. That the decision tree classifier and support vector machines are used in order to achieve high performance. They are very low-cost method because it features easily be extracted from the header. In YE et al,[7] are check full of forms-based methods used to analyze the date, return addresses, ID message, RECIVED, FROM, TO, X_MAILER. Then Support Vector Machine used for classification.

- Content based techniques utilizing feature extraction and image content analysis .

This type of filters to analyze and study their picture content and features such as color, edge, texture, etc are extracted from the image that expresses the general characteristics of image spam.
In Kim et al,[8] proposed a new approach to visual communication called BLASTed, to detect closest duplicate image is used. They are characteristics of the 3 groups (based on the color, the texture, and semantic profile) have used, the algorithm sequence of genes to detect similarities between the 2 images were used. In Gao et al,[2] to simulate real process of identifying spam on the Internet, a system based on learning ISH (Image Spam Hunter) provided. The proposed system classified the spam images collected by image similarity measure with



K_Means method according to color and histogram features. Then on of machine learning algorithms, Probability Boosting Tree (PBT) , to detect spam from non-spam input images based on the color histogram and histogram features to be used. In AL_Duwair et al,[1] presented a method and called Image Texture Analysis-Based Image Spam Filtering (ITA_ISA). used lowlevel features for the characters and then extracts the image features and used classifiers such as C4.5 Decision tree and Support Vector Machine (SVM) to categorize them. Mohanaiah et al,[9] in order to obtain the statistical properties of the texture image, GLCM have been used. GLCM is a second order statistical feature extraction method in this paper is used for motion estimation in images. The four feature, Entropy , energy, correlation, homogeneity were used.

• OCR based techniques utilizing OCR (Optical Character Recognition) and process text.

Generally OCR system as a translator for images that include handwriting, line types, or text printed is defined. Spam filtering used OCR techniques to extract text from images. After extracting text to analyze it pays to find keywords that are associated with spam images. Then image to be determined as spam or non-spam. Sometimes this method was successful, but recently most manufacturers use different obfuscation techniques that obscure the spam image causing anti-spam filters, inefficiency. In the first study OCR is the best options for filtering image spam , but the second issue to consider. First, High computational cost when processing image spam filtering and, secondly, that OCR is very vulnerable and the spammer would use a different trick. Although OCR on some tricks successful, but success in some of them is very difficult and OCR cannot function properly despite them. Because every time OCR in order to overcome these problems updates, this makes increases the computational cost. In 2005 and before, any text obfuscation techniques to attach images by spammers was not used. But OCR Applications to detect image spam obfuscation techniques used in cases where there is no applications.[10]

3. The proposed method:

In this paper, a new method for the detection of spam images provided using GLCM extracted 22 image features. then classifies the image, Using machine learning classifier.

3.1. GLCM

Texture is a characteristic sight of the surface and is an important characteristic to describe the different parts of the image. The purpose of the study of texture to find a way to describe the basic features of the image and displays them in a single and simple form which can be used to accurately classify. Image texture features are calculated using probabilistic properties.in this Features, One dimension based on the gray level intensity histogram. 2 dimensional Features is based on GLCM. This method is widely used in the analysis of image texture and show the number of event that different combinations of pixel brightness level occurred [11].

GLCM matrix is a second order method to provide image texture features. In this way,this method specifies, the conditional probability of all paired combinations pixels of gray levels in a framework of spatial the image varies according to the distance between pixels (d) and orientation (ɵ).The number of rows and columns of the matrix is equal to the number of gray levels in the original image that the resulting matrix show with p (i, j | d,ɵ), where d = (1,2,3, ...) and ɵ = (0,45,90,135) and also the number of gray levels of the matrix can be equal (8, 16,32.64.128.256)[12]. In this study, the distance between the pixel and the orientation are considered by default, ɵ = 0 and d = 1. Then number of levels was considered for matrix is 64. After using this matrix, 22 features can be obtained for each image is shown in Table 1. The number of Obtained features, including energy, entropy image, homogeneity, difference inverse correlation between pixels, a contrast image pixel intensity, the total variance, and so on. The parameters used in this specification is shown in Table 2.

4. Performance evaluation

4.1.described Performance metrics

If multiple images have the same characteristics (even common), Pictures of spam filtering techniques may be to identify with these images ,make mistakes. so an evaluation criterion for the way in this area is recommended. True positive (TP), false positive (FP), true negative (TN), false negative (FN), they are 4 quantity in the field of spam and to compare different methods that have been used by researchers. Classification for filtering image spam is used to categorize images. In order to measure the performance of the classifier, if the test image data to be identified as spam, this means that spam detection test results were positive and if the image is identified as non-spam or valid picture, it means that the test result is negative. So identified as follows[15]:

1- True positive (TP): This measure indicates that an image spam is correctly classified as spam.
2- False positive (FP): This measure indicates that this is a valid image or non-spam wrongly classified as spam.
3- True negative (TN): This measure indicates the valid image or non-spam image is correctly classified as non-spam image.
4- False negative (FN): This measure indicates that the image spam wrongly classified as non-spam images.

The more detail by researchers to evaluate the methods proposed formulas used to identify spam that briefly explain them.

- $Accuracy = \frac{(T_P+T_N)}{(T_P+T_N+F_P+F_N)}$

- $precision = \frac{(T_P)}{(T_P + F_P)}$
- $Recall = \frac{(T_P)}{(T_P + F_N)}$
- $F1 - measur = 2 * \frac{(Precision * Recall)}{(Precision + Recall)}$

- Table1: Features extraction from each image

features			features		
F1	Autocorrelation	$\sum_i \sum_j (i \cdot j) p(i,j)$	F12	Maximum probability	$\max_{ij} p(i,j)$
F2	Contrast	$\sum_i \sum_j \lvert i-j \rvert^2 p(i,j)$	F13	Sum of squares	$\sum_i \sum_j (i-v)^2 p(i,j)$
F3	Correlation I	$\sum_i \sum_j \frac{(i-\mu_x)(j-\mu_y)p(i,j)}{\sigma_x \sigma_y}$	F14	Sum average	$\sum_{i=2}^{2L} i \cdot p_{x+y}(i)$
F4	Correlation II	$\sum_i \sum_j \frac{(i \cdot j)p(i,j) - \mu_x \mu_y}{\sigma_x \sigma_y}$	F15	Sum entropy	$-\sum_{i=2}^{2L} p_{x+y}(i) \cdot \log(p_{x+y}(i))$
F5	Cluster prominence	$\sum_i \sum_j (i+j-\mu_x-\mu_y)^4 p(i,j)$	F16	Sum variance	$\sum_{i=2}^{2L} (i-F15)^2 \cdot p_{x+y}(i)$
F6	Cluster shade	$\sum_i \sum_j (i+j-\mu_x-\mu_y)^3 p(i,j)$	F17	Difference variance	$\sum_{i=0}^{L-1} i^2 \cdot p_{x-y}(i)$
F7	Dissimilarity	$\sum_i \sum_j \lvert i-j \rvert \cdot p(i,j)$	F18	Difference entropy	$-\sum_{i=0}^{L-1} p_{x-y}(i) \cdot \log(p_{x-y}(i))$
F8	Energy	$\sum_i \sum_j p(i,j)^2$	F19	Information measure of correlation I	$\frac{HXY - HXY1}{\max(HX, HY)}$
F9	Entropy	$-\sum_i \sum_j p(i,j) \cdot \log(p(i,j))$	F20	Information measure of correlation II	$(1-\exp[-2(HXY2 - HXY)])^{1/2}$
F10	Homogeneity I	$\sum_i \sum_j \frac{p(i,j)}{1+\lvert i-j \rvert}$	F21	Inverse difference normalized	$\sum_i \sum_j \frac{p(i,j)}{1+\lvert i-j \rvert^2 / L}$
F11	Homogeneity II	$\sum_i \sum_j \frac{p(i,j)}{1+\lvert i-j \rvert^2}$	F22	Inverse difference moment normalized	$\sum_i \sum_j \frac{p(i,j)}{1+(i-j)^2 / L}$

Table2: Parameters used

variable		variable	
$p_x(i)$	$\sum_{j=1}^{L} p(i,j)$.		
$p_y(i)$	$\sum_{i=1}^{L} p(i,j)$.		
μ_x	$\sum_i \sum_j i \cdot p(i,j)$.	HX	$-\sum_i p_x(i) \cdot \log(p_x(i))$.
μ_y	$\sum_i \sum_j j \cdot p(i,j)$.	HY	$-\sum_i p_y(i) \cdot \log(p_y(i))$.
σ_x^2	$\sum_i \sum_j (i-\mu_x)^2 \cdot p(i,j)$.	HXY	$-\sum_i \sum_j p(i,j) \cdot \log(p(i,j))$.
σ_y^2	$\sum_i \sum_j (j-\mu_y)^2 \cdot p(i,j)$.	$HXY1$	$-\sum_i \sum_j p(i,j) \cdot \log(p_x(i)p_y(j))$.
$p_{x+y}(k)$	$\sum_{i=1}^{L} \sum_{\substack{j=1 \\ i+j=k}}^{L} p(i,j)$, $k = 2,3,\ldots,2L$.	$HXY2$	$-\sum_i \sum_j p_x(i)p_y(j) \cdot \log(p_x(i)p_y(j))$.
$p_{x-y}(k)$	$\sum_{i=1}^{L} \sum_{\substack{j=1 \\ \lvert i-j\rvert=k}}^{L} p(i,j)$, $k = 0,1,\ldots,L-1$.		

Accuracy measure is to say the number of correctly identified spam images as well as images that are compared all images marked valid [13]. precision, or True Positive rate(TP), is a measure of the rate of spam images were classified correctly as compared to the total amount of spam images correctly classified. Recall , indicating rate of spam images, which are correctly classified as spam compared with all the images of spam and non-spam that correctly classified. F1 measure, This measures the weighted average rate of Recall and Precision.

4.2.Datasets

In this study, two data sets were used that it contains spam image and non-spam, which is mainly used for evaluation of image spam filtering techniques.

1. Dredze Dataset[14]: This dataset contains only images that are valid and non-valid emails extracted and the data includes 2021 images and 3299 non-spam spam images.
2. Image Spam Hunter ISH Data set[2]: This dataset contains 810 non-spam images that randomly were collected from Flicker.com and 926 images spam is used which is collected from the actual e-mail.

Results

In this study, using the image datasets listed, after the mentioned features are extracted from each image, to classify the images and results according to the listed evaluation criteria, offered in this section. Classifying them according to machine learning classifier, such as the K-Nearest Neighbor (KNN) and Bayesian Network (BN) have been done. Datasets , divided into training set and test sets that is according to the methods of cross validation. In this paper has been used 5_fold cross validation. Results are shown in Table 3. Compare the results of two datasets can be deduced that the results is ISH dataset, is better than Dredze dataset. In this dataset, there are images with no textures, advertising logo and invalid files, because the results have been less than ISH datasets. The articles related to this dataset, delete this data

before processing is expressed. Compare these results with other cases in which there shows that mentioned method have better action in section reducing system processing time, and the accuracy of the results as compared to existing methods.

Conclusion

In this article, a method to detect images spam from non-spam images were introduced. using of GLCM matrix that is one of image texture features, for every image, 22 statistical parameters textures was achieved such as energy, entropy, contrast and etc. Result obtained of Classification images, show an improvement in the Categories the images and reduce time as compared to previous work.

Table3: The results

Datasets	Performance evaluation	Classifying	
		KNN	NB
Dredze	Acc: Prec: Rec: F-Meas:	91/41 87/03 99/53 92/86	75/49 78/98 82/12 80/52
ISH	Acc: Prec: Rec: F-Meas:	93/74 97/96 91/01 94/35	99/19 100/00 98/52 99/25

References:

Al-Duwair,B. ,Khater,I. ,Al-Jarrah.O. Detecting Image Spam Using Image Texture Features ,International Journal for information security Research(IJISR),Volume2,Issues3/4,2012, pp.344-353

Attar,A.,Moradi rad,R.,Ebrahimi,R.2013." A survey of image spamming and filtering techniques",Springer Science Business Media,Artif Intell Rev,71-105.

Biggio,B.,Fumera,G.,Pillai,I.,Roli,F.2007." Image spam filtering using visual information" .In:14th Internat.Conf. Image Anal. Process. IEEE Computer. Society ,pp,105–110.

Dredze ,M., and Bachrach,.A. 2007. "Learning Fast Classifiers for Image Spam," presented at the in Proc. CEAS 2007, Mountain View, California, August 2-3.

Gao, Y. , Yang , M., Zhao,X. 2008. "Image Spam Hunter," in Acoustics, Speech and Signal Processing,ICASSP 2008. IEEE International Conference on, pp. 1765, 1768.

Gao,Y., Yang,M., Choudhary,A. 2009. "Semi supervised image spam hunter: aregularized discriminant EM approach." In: The international conference on advanced data mining and applications (ADMA) China.

He,P.,Wen,X.,Zheng,W.2009."A simple method for filtering image spam".In:IEEE/ ACIS Int. Conf.Comput.Inf.Sci., ,pp.910–913.

Hu,S.,Xu,C.,Guan,W.,Tang,Y.,Liu,Y.2014." Texture feature extraction based on wavelet transform and gray-level co-occurrence matrices applied to osteosarcoma diagnosis ".

Kim,H.,Chang,H.,Lee,J.,Lee,D.2010."BASIL:effectivenear-duplicate image detection using gene sequence alignment".In: 32nd European conference on information retrieval , Springer,UK

Krasser,S., Tang,Y., Gould,J., Alperovitch,D., Judge,P., 2007. " Identifying image spam based on header and file Properties using C4.5decision trees and support vector.

Mehta, B., Nangia, S. , Gupta, M. , Nejdl, W. 2008. "Detecting Image Spam Using Visual Features and Near Duplicate Detection," In Proceeding of the 17th international conference on World Wide Web, Beijing, China.

Mohanaiah,P.,Sathyanarayana,P.,Gurukumar,L.2013."Image Texture Feature Extraction Using GLCM Approach". International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013 .

Saraubon ,K., Limthanmaphon,B. 2009 ."Fast effective botnet spam detection. " In: Fourth international conference on computer sciences and convergence information technology,Korea

Sebastian,B.,Unnikrishan,A.,Balakrishnan,K.2012."Grey Level Co-occurrence Matrices: Generalisation And Some New Features". International Journal of Computer Science, Engineering andInformation Technology (IJCSEIT), Vol.2, No.2, April 2012.

Ye,M., Tao,T., Mai,FJ., Cheng,XH. 2008. "An spam discrimination based on mail header feature and SVM". In: The 4th international conference on wireless communications.