

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed* and Noor Basim Bethoon**

*University of Technology-computer Sciences department

**University of Technology-chemical engineering department

Received 25 July 2016 ; Accepted 3 October 2016

Abstract

The rapid advancement of mobile phone systems and programs that support free Instant messaging (IM), short messaging services (SMS), and the convenience of sending millions of messages with practically no delay and almost zero cost, through WIFI or 3G has led to the increasing popularity of short messaging services . The requirement is an automatic classification system for quick classification for the received messages. . in order to detect the suspicious message .In this paper we use detection model in which social media messages are classified as a predefined classes named suspicious and not suspicious .The proposed system try achieved this problem through simple method known as level based feature content . In this method the content feature is divided into four levels to detection suspicious.This system works offline , collecting the message online , save it and then input to the proposed system.The experimental result show that the level three detection rate is higher than the rest levels with accuracy 0.952381 when the threshold 0.06 and to improvement the overall levels results of the system we use the majority test, where the accuracy reached to 100%

Keywords: classification, instant message,suspicious,non suspicious, viber, level of features,

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

نموذج بسيط لكشف رسائل الفايبر المشبوهة

هناك محسن احمد* و نور باسم بيثون**
 *الجامعة التكنولوجية - قسم علم الحاسوب
 **الجامعة التكنولوجية - قسم الهندسة الكيماوية

الخلاصة

كان للتقدم السريع الذي اجتاحت انظمة الهواتف النقالة و البرامج التي تدعم ارسال الرسائل المجانية، و خدمات الرسائل القصيرة عبر الهاتف، فضلا عن سهولة ارسال ملايين الرسائل من دون تأخيرا و بكلفة تناهز الصفر عبر شبكات الواي فاي و 3جي، كان هذا السبب لزيادة شعبية خدمات الرسائل الى حد كبير. ظهرت الحاجة الى نظام تصنيف الكتروني للتصنيف السريع للرسائل المستلمة. ضمن هذا البحث، نستخدم نموذج للكشف بغية تصنيف رسائل و سائط التواصل الاجتماعي الى فئات معروفة مسبقا (مثيرة للشكوك و غير مثيرة للشكوك) حيث يحل النظام المقترح هذه المشكلة عبر طريقة بسيطة تعرف بمستويات بالاعتماد على مميزات محتوى الرسالة حيث يتم تقسيم المميزات الى اربعة مستويات للكشف عن الرسائل المثيرة للشكوك و النظام يعمل بصورة (off line) يتم جمع الرسائل (online) و خزنها و ادخالها الى النظام المقترح و النتائج العملية اظهرت على ان دقة المستوى الثالث أعلى من المستويات البقية حيث وصلت الى 95.23 عند عتبة 0.06 و لتحسين النتائج الإجمالية للنظام تم استخدام اختبار الأغلبية حيث اظهرت النتائج ان دقة المصنف باستخدام المستويات الاربعة وصلت الى 100%

الكلمات المفتاحية: تصنيف، الرسائل الفورية، مثيرة للشكوك ، غير مثيرة للشكوك ، مستويات الخصائص

Introduction

As majority information (more than 80%) is stocked as text. Text mining is thought to have a high value of commercial potential , discovering of knowledge may be from a lot of number of information sources , unstructured texts still the biggest easy source of the availability of knowledge .Text classification which classifies the documents according to predefined categories.[1]Text mining is a modern field of computer science which promote, strong dealings with natural language processing (NLP), machine learning (ML), information retrieval (IR), Data mining (DM), and knowledge management (KM). Text mining attempt to extract useful information from unstructured textual data through determining and exploring exciting patterns [2] SMS and IM have specific characters that may unlike the characters of mails . A mail divided to number of fields such as Address of senders subject of message header mail ,

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

etc, While IM and SMS don't have such fields. This is the reason of the difficulty of the task of SMS and IM classification.that lead to necessity of improveing method of filtering. [3]Today, most approaches to text classification are based on the bag-of-words representation where a document is mapped to a vector of word counts. While easy to compute and manipulate, this representation ignores relations across different sentences in text and disregards the underlying structure of a document. All message are converted into text documents. [4]Suspicious message is the message that sent electronically and it unwanted. Email suspicious messages are transfer over the Internet while SMS and IM suspicious are send / received over a mobile network, viber message suspicious is typically transmitted over 3G or WiFi. Viber is an instant messaging and Voice over IP (VoIP) application for smart phones developed by Viber Media. [5]The Islamic State of Iraq and Syria (ISIS), a militant Jihadist organization, use viber service to communicate. [6]

The paper is organized as follows: Section one introduction, Section two summarize the related work done using various method for classification, Section three gives a general theoretical description on Text Categorization and its applications, SMS classification, Morphology, Viber application, ROC curve , Majority ,Section four Present detailed steps of the proposed system and performance comparison of the four levels of feature in section five make Ehmancement to the Result, finally we closed the paper with the conclusion in section six.

Related Work

Unlike the growing and large number of papers about email spam classifiers the research about SMS (short message service) spam filtering Interests are still a few in this area, amount of junk SMS and email are increasing every day junk SMS amount is more than the email , there are many people this domain (suspicious detection) on email message and SMS, below relevant works related to this topic

- **Almeida et-al** in (2011) they displayed a new real , public and non encoded SMS spam collection that is the bigger one in so far as they know in addition , they compare the performance achieved by several established machine learning methods , they found that

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

support vector machine gives good result compared with other classifier and hence it can be used as a good base line for further comparison.[7]

- **Patel,Bhatnagar**,in(2011)propose a model that first use the entropy term weighting scheme and then PCA is used for the reparameterization. after that used the ANN (artificial neural network) for classification. that model may be successful in efficiently classifyingSMS text document implementation of this model will be further in future[8]
- **Shirani-Mehr**, in(2012)they usedreal SMSdatabase (UCI machine learning repository) began with step of preprocessing and feature extraction after that apply different machine learning algorithm to SMS spam classification problem and found the best result founded from the used of SVM as the learning algorithm which yields overall accuracy of 97.64%. [9]
- **Eshmawi and Nairin** (2013) they injected new features based on domain knowledge and study the possibility of using the few number of optimal features to classify SMS spam messages .The result achieved best from BOW approaches that use many number of features.[10]
- **Shahi and Yadav** in (2014) they used, the SVM-based and Naïve Bayes classification techniques are execute to classify the Nepali SMS as Spam and non-Spam. the empirical analysis for diffrent sample of text has been done to measure the accuracy of the classification methodologies used in this study. and, it is found to be 87.15% accurate in SVM and 92.74% accurate in the case of Naïve Bayes. [3]

Text Categorization

Text Categorization(TC), can called as text classification, text document automaticly classification under previously determined classes .

Machine Learning (ML) and information Retrieval (IR) mechanism, are used to appoint words that called (attributes,features,terms,tokens) to the documents and classifying them into specific classes .The benefit of performing text classification is multifold. Obviously, text classification can reduce the cost and time of human-effort for labeling documents, which also reduces the probability of making errors during labeling . [11]Text classification is arguably

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

one of the most important research areas of text mining and machine learning. Applications of text classification include many research fields, such as query classification email spam filtering .[12]

1-The Text Groups Applications

The main applications of the text categorization(TC) are explained in the following sections:[13]:

Automatic Indexing, Document Organization, Hierarchical Web Page Categorization, Document Filtering, Word Sense Disambiguation

2- SMS Classification

SMS, IM of viber suspicious have caused mobile device users and mobile network operators a lot of problems. Suspicious messages Disturbs users by filling their storage and wastefulness time reading and deleting suspicious messages.[14]

For SMS classification their are two types Black and White filters ,these method are based on patterns and keywords that are previously known.[15]

The few number of filtering program for phone mobile led to detection spam in text message interesting issue to look into.

A number of major differences exist between spam-filtering in text messages and emails. Unlike emails, which have a variety of large datasets available,the real suspicious databases for SMS and IM for social network applications are very limited.

Additionally, due to the small length of text messages, the number of features that can be used for their classification is far smaller than the corresponding number in emails.[9]

3- Morphology

Types of morphology are two the first one analyzing a word and the second using for generation a word .[16]

here we are transact with the morphology that can analyzing a word (English Word).

In english language the morphology dealing with the changes that happen through adding affixes to the words (such as rot will be rotting and go will be going by adding "ing").

prefixes and suffixes are the types of affixes In English language.[17]

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

4- Viber Application

Everyone in the world can connect freely with viber. Viber has more than 664 million users worldwide sending messages and making HD-quality phone and video calls over WiFi or 3G - for free.[18] You can create group messages with up to 200 friends, share photos, video, stickers, links and more. There's no need to register – your phone number is your ID and Viber syncs with your mobile contact list automatically.[19]

Viber properties follow as : [20]

1. Message your friends (texts can be up to 7,000 characters long).
2. Make free phone and video calls with HD sound quality.
3. Share photos, videos, voice messages, locations, contact info, rich links, stickers and emoticons .
4. Attach files – send messages with documents, presentations, archives and most other files via Viber.
5. Delete a message from all members of the conversation, even after it's been sent.
6. Support for the viber desktop application on Windows, Mac, Linux and Windows 8

5- ROC Curve

Its graph that used usually that recap the classifier performance over all thresholds conceivable . It is plotting the False Positive Rate (x-axis) and True Positive Rate (y-axis) as you vary the threshold for assigning observations to a given class..[21]

6-Majority

A majority is the greater part, or more than half, of the total. It is a subset of a set consisting of more than half of the set's elements[22]

Proposal Methodology

The evolution of social media techniques and programs are bringing newer security concerns to Internet users and network administration . These concerns are in general stemming from the unsolicited and malicious information being send to the users. The resulting damage has been seen in the form of excess data usage, network load trouble, secret information stealing , denial-of-service attacks and other cyber-crimes.

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

For this reason there was a need for program dealing with these suspicious messages.

In this paper we present a method for building detection system to find a (suspicious features) in the IM of Viber.

However, we need to collecting instant message(Viber) using CopyTrans Control Center program , working online in collecting message and downloading it as text file , and then the system working offline the step of preprocessing , and then test the text in four levels of feature by matching text with the features we store in database and the result determined the type of message and use the majority to improve the result and use ROC curve to test results from four levels evaluation and find level two badly result

1- Message Documents Collect

The main method to collect instant message data(Viber message) is to ask mobile users to contribute text messages voluntarily because there is no such benchmark instant message dataset available in the counter terrorism domain .

This method has been used primarily to collect legitimate SMS text messages for research. All messagetexts for training and testing are monolingual English written texts.below some example ofnon suspicious messages and suspicious in tables 1,2

Table (1): sample of non suspicious message

Non suspicious message	
1	Baghdad - Iraqi Prime Minister Haider al-Abadi called on Saturday for legal action over allegations that senior officials took millions of dollars in bribes to help major firms secure lucrative oil sector contracts.
2	Obama said, "tell us the person who made the statements doesn't know much about foreign policy or nuclear policy or the Korean peninsula or the world generally".
3	Czech Interior Minister Milan Chovanec says authorities in Prague will send a group of Iraqi Christians back to Iraq after they tried to move to Germany rather than staying in the Czech Republic. About 25 Iraqis took a bus to Germany on April 2 but were stopped by German police immediately after crossing the border.

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

Table (2): sample of suspicious message

	suspicious message
1	Syria war: 'Islamic State' loses al-Qaryatain to government forces Syrian forces and their allies have retaken the central town of al-Qaryatain from so-called Islamic State (IS), dealing a further strategic blow to the militant group, state media say. It comes days after IS was pushed out of the nearby ancient city of Palmyra.
2	Terrorist groups, most notably ISIL, on a mass scale committed acts of violence ,including killing by means of suicide bombings, improvised explosive devices ,execution-style shootings, and beheadings. These groups also engaged in kidnapping, rape, and other forms of violence.
3	For the first time since deadly terrorist bombings rocked Brussels, the city's main airport on Sunday will reopen to passengers -- albeit to a very limited number of them

1.1 Process of Message Classification

To classify the text documents first we determine the suspicious features and store in database and then pre-processing is applied as shown in figure(1). This process objective is to decrease the document spaces state and clean the text message

All dataset go through a pre-processing phase. The training data set goes through all steps of the preprocessing phase, while the documents to be classified (testing data) go through tokenization to matching feature only as shown in Figure (1).

- a) **Tokenization:** "Is the process of breaking a stream of text into words, phrases, symbols, or other meaningful elements called tokens .The aim of the tokenization is the exploration of the words in a sentence. The list of tokens becomes input for further processing such as parsing or text mining".[24]
- b) **Normalization :**"Convert words into a normalized forms – down-case, e.g. The = the, NF-kappa B = nf-kappa b"[25]

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

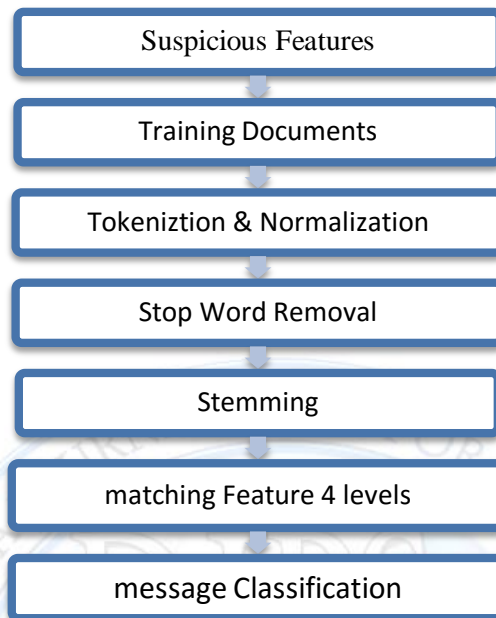


Figure (1) : Message Classification Process

- c) **Removing Stop Words:**"Stop words such as “the”, “a”, “and”, etc are frequently occurring, so the insignificant words need to be removed. This process also reduces the text data and improves the system performance. Every text document deals with these words which are not necessary for text mining applications.[26] show in table (3) sample of stop word" .[27]

Table (3): sample of stop wordusing in message processin

a	able	about	across	after	all	almost
also	am	among	an	and	any	are
as	at	be	because	been	but	by
can	cannot	could	dear	did	do	does
either	else	ever	every	for	from	get
got	had	has	have	he	her	hers
him	his	how	however	i	if	in
into	is	it	its	just	least	Let
like	likely	may	me	might	most	must
my	neither	no	nor	not	of	off
often	on	only	or	other	our	own
rather	said	say	says	she	should	since

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

- d) **Stemming Word:** This technique transforms words into their stems, which generalizes the texts for similarity analysis .For this step ,a process of conflating tokens to their rootform.for example, both “computer” and “computers” are normalized to “comput”, and “product”, “produce”, and “produced” to “produce”, and " connection" to connect, computing to compute.[28]
- e) **Matching Features :** Split the levels of feture to four levels
- I. **Level One:**If find one or more of important featuresin message that's mean the message is suspicious .table (4) show some of important features

Table (4): sample of Important features using in matching features

Important features	المعنى	Important features	المعنى	Important features	المعنى
Bomb	قنبلة	Attack	هجوم	Daesh	داعش
Isis	الدولة الاسلاميه في العراق والشام	AQI	تنظيم القاعدة في العراق	Kill	قتل
C4	غاز يستخدم في صناعه المتفجرات	Isil	الدولة الاسلاميه في العراق	Behead	قطع رأسه
Gang	عصابة	W.M.D	اسلحة دمار شامل	Blaster	الناسف
Terrorist	إرهابي	Genocide	إبادة جماعي	Crime	جريمة
Daish	داعش	Explosion	انفجار	Decapitate	ضرب العنق

- II. **Level Two:** Search for features that have two word if feature consists of two parts must search for two part and matching that if find one feature not necessarily be wholesale suspicious **ex.Islamic state** if find Islamic not mean message is suspicious or find **state** that not mean issuspicious but if find **Islamic state** that mean is message is suspicious . table (5) show some of tow word feature

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

Table (5): sample of two words feature using in matching features

Two words feature	المعنى	Two words feature	المعنى	Two words feature	المعنى
Islamic State	الدولة الإسلامية	explosive belt	حزام ناسف	unidentified body	جثة مجهولة الهوية
terrorist group	جماعة ارهابية	islamic terrorisim	الإرهاب الإسلامي	al_qaeda mititants	متمشددى القاعدة
armed group	مجموعة مسلحة	repressive measures	اجراءات قمعيه	sunni extremists	المتطرفون السنة
al Baghdadi	البغدادي	religious extremism	التطرف الديني	terrorist organization	منظمه ارهابية
nuclear security	الأمن النووي	assassination attempt	محاولة اغتيال	time bomb	قنبلة موقوتة

III. **Level Three** :Matching the content of message with the all suspicious features and if find two or more of features in message that mean message is suspicious.table (6) show some of suspicious features

Table (6): sample of suspicious feature using in matching features

Suspicious features	المعنى	Suspicious features	المعنى	Suspicious features	المعنى
operate	العمليات	raid	غارة	resist	مقاومة
terrorist	الأرهابية	launch	يشن	Opponent	الخصم
extremist	المتطرفة	mount	يشن	Repress	القمع
Kill	القتل	beheadings	قطع الرؤوس	Secure	الامن
kidnap	الخطف	storm	يهاجم /ينقض على	Annihilate	اباد
bomb	التفجيرات	flee	هرب	Combat	مكافحة

IV. **Level Four**:Matching the content of message with the all suspicious features and if find (number of feature / number of token in message > threshold) that mean message is suspicious doing that by using The ROC curve corresponds to the graphical representation of the couple (1 – specificity, sensitivity) for the various possible threshold values. and find the best threshold is **0.06** figure (2) show the best value of threshold The ROC analysis table find Sensitivity, Specificity, TP, TN, FP, FN depending on the value of the threshold value.as show in table (7)

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

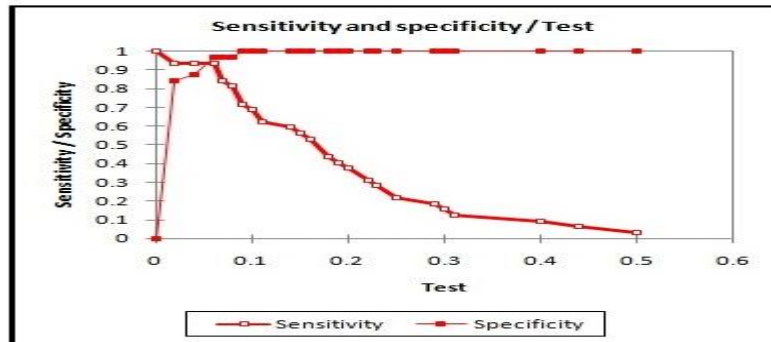


Figure (2) : The Best Value Of Threshold

Table (7): The ROC analysis table

Test	Sensitivity	Specificity	TP	TN	FP	FN	Sensitivity+ Specificity	Accuracy
0.000	1.000	0.000	32	0	32	0	1.000	0.500
0.020	0.938	0.844	30	27	5	2	1.781	0.891
0.040	0.938	0.875	30	28	4	2	1.813	0.906
0.060	0.938	0.969	30	31	1	2	1.906	0.953
0.070	0.844	0.969	27	31	1	5	1.813	0.906
0.080	0.813	0.969	26	31	1	6	1.781	0.891
0.090	0.719	1.000	23	32	0	9	1.719	0.859
0.100	0.688	1.000	22	32	0	10	1.688	0.844
0.110	0.625	1.000	20	32	0	12	1.625	0.813
0.140	0.594	1.000	19	32	0	13	1.594	0.797
0.150	0.563	1.000	18	32	0	14	1.563	0.781
0.160	0.531	1.000	17	32	0	15	1.531	0.766
0.180	0.438	1.000	14	32	0	18	1.438	0.719
0.190	0.406	1.000	13	32	0	19	1.406	0.703
0.200	0.375	1.000	12	32	0	20	1.375	0.688
0.220	0.313	1.000	10	32	0	22	1.313	0.656
0.230	0.281	1.000	9	32	0	23	1.281	0.641
0.250	0.219	1.000	7	32	0	25	1.219	0.609
0.290	0.188	1.000	6	32	0	26	1.188	0.594
0.300	0.156	1.000	5	32	0	27	1.156	0.578
0.310	0.125	1.000	4	32	0	28	1.125	0.563
0.400	0.094	1.000	3	32	0	29	1.094	0.547
0.440	0.063	1.000	2	32	0	30	1.063	0.531
0.500	0.031	1.000	1	32	0	31	1.031	0.516

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

1.2 Evaluation metrics

Text classification rules are typically evaluated using performance measures from information retrieval. Common metrics for text categorization evaluation include recall, precision, accuracy and error rate and F1. Given a test set of N documents, a two-by-two contingency table with four cells can be constructed for each binary classification problem. The cells contain the counts for true positive (TP), false positive (FP), true negative (TN) and false negative (FN), true positive rate (TPR), false positive rate (FPR) respectively.[29]

True Positives (TP) = the number of cases which were correctly classified to be positive, i.e. were predicted to be a success and were actually observed to be a success.[30]

False Positives (FP) = the number of cases which were incorrectly classified as positive, i.e. were predicted to be a success but were actually observed to be a failure .[30]

True Negatives (TN) = the number of cases which were correctly classified to be negative, i.e. were predicted to be a failure and were actually observed to be a failure.[30]

False Negatives (FN) = the number of cases which were incorrectly classified as negative, i.e. were predicted to be a negative but were actually observed to be a success.[30]

Clearly, $N = TP + FP + TN + FN$. The metrics for binary-decisions are defined as:

- Accuracy = $(TP + TN)/N$: is the ratio between the number of text documents which were correctly categorized and the total number of text documents.[31]
- Error = $(FP + FN)/N$: is the ratio between the number of text documents which were not correctly categorized and the total number of text documents:.[31]
- Precision = $TP / (TP + FP)$: is the percentage of correctly categorized text documents among all text documents that were assigned to the category by the classifier.[31]
- Recall = $TP / (TP + FN)$ is the percentage of correctly categorized text documents among all text documents belonging e the score: p is the number of correct positive results divided by the number of all positive results, and r is the number of correct positive results divided by the number of positive results that should have been returned. The F1 score can be interpreted as a weighted average of the precision and recall, where an F1 score reaches its best value at 1 and worst at 0.[31]

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

- $F1 = \frac{2 * Recall * Precision}{Recall + Precision}$: is a measure of a test's accuracy. It considers both the precision p and the recall r of the test to compute.[32]
- $TPR = \frac{TP}{TP+FN}$ True Positive Rate : The fraction of positive target that are classified as positive[33]
- $FPR = \frac{FP}{FP+TN}$ False Positive Rate: The fraction of negative examples (No, False, -) that are classified as positive (Yes, True, +)[33]

Experiment Results

- **Level one: Find Important Feature**

Table (8): Level One Result

Accuracy	0.890625
Error	0.109375
Precision	0.96296296
Recall,TPR, Sensitivity	0.8125
FPR	0.03125
F1	0.881355931

Table (9) Classification confusion matrix “Level one Important Feature”

Classification confusion matrix		
	Actual class	
Predicated class	sus	no
sus	26(TP)	1(FP)
no	6(FN)	31(TN)

- **Level Two: Feature consist of two words**

Table (10): Level Two Result

Accuracy	0.609375
Error	0.390625
Precision	1
Recall,TPR, Sensitivity	0.21875
FPR	0
F1	0.358974359

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

Table (11) Classification confusion matrix “Level two Feature Consist of Two Words

Classification confusion matrix		
Predicated class	Actual class	
	sus	no
sus	7(TP)	0(FP)
no	25(FN)	32(TN)

- Level three: Test by threshold

Table (12): Level Three Result

Accuracy	0.953125
Error	0.046875
Precision	0.967742
Recall,TPR, Sensitivity	0.9375
FPR	0.03125
F1	0.952381

Table (13) Classification confusion matrix " level three for feature"

Classification confusion matrix		
Predicated class	Actual class	
	sus	no
sus	30(TP)	1(FP)
no	2(FN)	31(TN)

- Level four : Find two or more features

Table (14): Level Three Result

Accuracy	0.937
Error	0.0625
Precision	0.966666667
Recall,TPR, Sensitivity	0.90625
FPR	0.03125
F1	0.935483871

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

Table (15) Classification confusion matrix " level four for feature"

Classification confusion matrix		
Predicated class	Actual class	
	Sus	no
sus	29(TP)	1(FP)
no	3(FN)	31(TN)

Table (16) summary result for four levels of feature

leve l	Magarit y weight	Accuracy	Error	Precision	Recall	F1
1	0.2	0.890625	0.109375	0.96296296	0.8125	0.881355931
2	0.1	0.609375	0.390625	1	0.21875	0.358974359
3	0.4	0.953125	0.046875	0.967742	0.9375	0.952381
4	0.3	0.9375	0.0625	0.966666667	0.90625	0.935483871

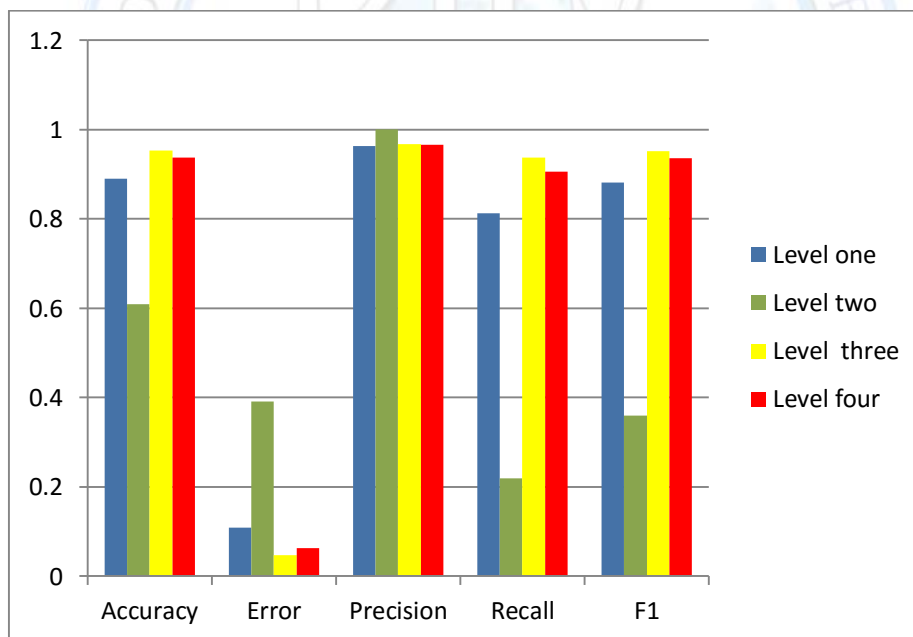


Figure (3) evaluation matricesFigure

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

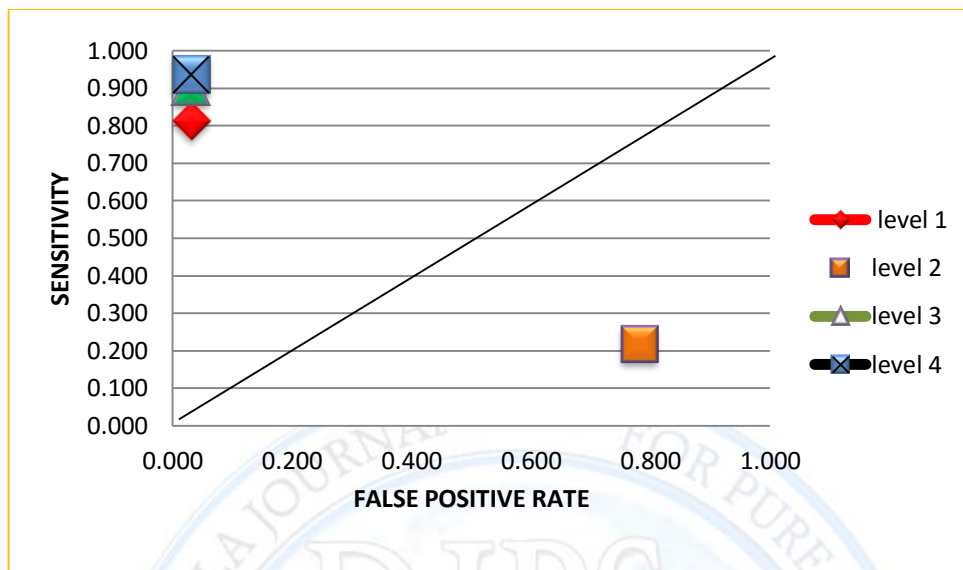


Figure (4) ROC Curve For Four Level Detection

Enhancement Results

To improvement the result uses majority test and give each level weight based on accuracy as show in table (17) Find the results of four levels and for more accuracy choose the result based on majority of the result offour levels we see in (table 18 .a ,b) the result of each level and the majority result where (T =True ,F =False, TW test weight)three of them need for more processing to decide the result because the result of levels test is two true and two false . based on weghit majority we can solve this proplem by calculation the weghit majority and if the over all result of four levels test more than 0.5 that mean theis message is true classification as its category under 0.5 that mean its classified is false

Table (17): weight and accuracy for level

level	Magarity weight	Accuracy
1	0.2	0.6258900.
2	0.1	0.609375
3	0.4	0.953125
4	0.3	0.9375

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

Table (18)majority of results (a .Suspicious ,b.non Suspicious)

a . suspicious

b. non suspicious

Weight level	Level 1	Level 2	Level 3	Level 4	Majority result	Weghit Majority	Level 1	Level 2	Level 3	Level 4	Majority result	Weghit Majority
	0.2	0.1	0.4	0.3			0.2	0.1	0.4	0.3		
1	T	F	T	T	T	0.9	T	T	T	T	T	1
2	F	F	T	F	F	0.4	T	T	T	T	T	1
3	T	F	T	T	T	0.9	T	T	T	T	T	1
4	T	T	T	T	T	1	T	T	T	T	T	1
5	F	T	T	T	T	0.8	T	T	T	T	T	1
6	T	F	T	T	T	0.9	T	T	T	T	T	1
7	T	F	T	T	T	0.9	T	T	T	T	T	1
8	T	F	T	T	T	0.9	T	T	T	T	T	1
9	T	F	T	T	T	0.9	T	T	T	T	T	1
10	T	F	T	T	T	0.9	T	T	T	T	T	1
11	T	F	T	T	T	0.9	T	T	T	T	T	1
12	T	F	T	T	T	0.9	T	T	T	T	T	1
13	T	F	T	T	T	0.9	T	T	T	T	T	1
14	T	F	T	T	T	0.9	T	T	T	T	T	1
15	T	F	T	T	T	0.9	T	T	T	T	T	1
16	T	F	T	T	T	0.9	T	T	T	T	T	1
17	F	T	F	F	F	0.1	T	T	T	T	T	1
18	T	T	T	T	T	1	T	T	T	T	T	1
19	F	F	F	F	F	0	T	T	T	T	T	1
20	T	T	T	T	T	1	T	T	T	T	T	1
21	T	F	T	T	T	0.9	T	T	T	T	T	1
22	T	T	T	T	T	1	T	T	T	T	T	1
23	T	T	T	T	T	1	T	T	T	T	T	1
24	T	F	T	T	T	0.9	T	T	T	T	T	1
25	T	F	T	T	T	0.9	T	T	T	T	T	1
26	T	F	T	T	T	0.9	T	T	T	T	T	1
27	T	F	T	T	T	0.9	T	T	T	T	T	1
28	F	F	T	T	TW	0.7	T	T	T	T	T	1
29	T	F	T	T	T	0.9	T	T	T	T	T	1
30	T	F	T	T	T	0.9	T	T	T	T	T	1
31	F	F	T	T	TW	0.7	T	T	T	T	T	1
32	T	F	T	T	T	0.9	F	T	T	F	TW	0.5

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

Conclusions

The task of detection suspicious (SMS or IM) still is a real challenge nowadays because the short came of real and public datasets , the message is full of idioms and abbreviations and few number of feature can find in each message . We have applied simple method to detect suspicious known as level based feature in this method the content feature is divided into four level to detection(suspicious, non-suspicious) to dataset of (64 messages suspicious and non-suspicious) and evaluates the performance of four levels of features and find the best performance of level three were shown in figures(3) It is clear that the best value of accuracy for more accuracy we can evaluate the four levels and then decide the result based on majority result from the four level and find the system become more accurate when to give weights for each level depend on the accuracy of each level.

Simple Detection Model to Suspicious Viber Messages

Hanaa Muhsin Ahmed and Noor Basim Bethoon

Reference

1. Korde, Vandana, and C. Namrata Mahender. "Text classification and classifiers: A survey." *International Journal of Artificial Intelligence & Applications* 3.2 (2012)
2. Radovanović, Miloš, and Mirjana Ivanović. "Text mining: Approaches and applications." *Novi Sad J. Math* 38.3 (2008): 227-234.
3. Shahi, Tej Bahadur, and Abhimanu Yadav. "Mobile SMS spam filtering for Nepali text using naïve bayesian and support vector machine." *International Journal of Intelligence Science* 4.01 (2013):.
4. Dzunic, Zoran. Text structure-aware classification. Diss. Massachusetts Institute of Technology, 2009.
5. internet survey Viber (2016) in Wikipedia. Available at: <https://en.wikipedia.org/wiki/Viber> (Accessed: 29 September 2016)
6. Internet survey , Reilly, R.B. and richard-byrne-reilly (2014) Viber now has 400M users, & many are using the service to survive in the war-torn middle east. Available at: <http://venturebeat.com/2014/07/30/viber-now-has-400m-users-many-are-using-the-service-to-survive-in-the-war-torn-middle-east/> (Accessed: 29 September 2016)
7. Almeida, Tiago A., José María G. Hidalgo, and Akebo Yamakami. "Contributions to the study of SMS spam filtering: new collection and results." *Proceedings of the 11th ACM symposium on Document engineering*. ACM, 2011.
8. Patel, Deepshikha, and Monika Bhatnagar. "Mobile SMS Classification." *International Journal of Soft Computing and Engineering (IJSCE) ISSN* (2011): 2231-2307.
9. HoushmandShirani-Mehr , " SMS Spam Detection using Machine Learning Approach", 2013
10. Eshmawi, Ala, and Suku Nair. "Feature reduction for optimum sms spam filtering using domain knowledge." *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2013.

Simple Detection Model to Suspicious Viber Messages**Hanaa Muhsin Ahmed and Noor Basim Bethoon**

11. Song, Yang. machine learning for text mining: classification. Diss. The Pennsylvania State University, 2009.
12. Kolcz, Aleksander, and Wen-Tau Yih. "Raising the baseline for high-precision text classifiers." Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2007.
13. Raymond J. Mooney, " Machine Learning Text Categorization" ,CS391L
14. Saeed, Hassan, and Waddah Waheeb. The performance of soft computing techniques on content-based SMS spam filtering. Diss. Universiti Tun Hussein Onn Malaysia, 2015.
15. Ahmed, Ishtiaq, Donghai Guan, and Tae Choong Chung. "Sms classification based on naive bayes classifier and apriori algorithm frequent itemset."International Journal of machine Learning and computing 4.2 (2014): 183.
16. Rahma, Abdul Monem S., Suhad M. Kadhem, and Alaa Kadhim Farhan. "Finding the Relevance Degree between an English Text and its Title." Eng. & Tech. Journal 30.9 (2012): 1625-1640.
17. Internet survey , Morphemes, roots and affixes (2011) Available at: <http://www.unizd.hr/Portals/36/kolegiji/morphology/Morphology%203.pdf> (Accessed: 29 September 2016).In-text citations: (Morphemes, roots and affixes, 201
18. Internet survey ,SarI, V.M. (2016) Viber on the App store. Available at: <https://itunes.apple.com/mr/app/viber/id382617920?mt=8>
19. Internet survey ,Viber (2015) Available at: <http://appcrawlr.com/ios/viber-free-phone-calls-text>
20. Internet survey ,GmbH, P.D. (2016) Viber - App store revenue & Download estimates. Available at: <https://prioridata.com/apps/viber-downloads-revenue-382617920>
21. Internet survey ,Data (2014b) Simple guide to confusion matrix terminology. Available at: <http://www.dataschool.io/simple-guide-to-confusion-matrix-terminology>
22. Internet survey ,Majority (2016) in Wikipedia. Available at: <https://en.wikipedia.org/wiki/Majority>

Simple Detection Model to Suspicious Viber Messages**Hanaa Muhsin Ahmed and Noor Basim Bethoon**

23. Dalal, Mita K., and Mukesh A. Zaveri. "Automatic text classification: a technical review." *International Journal of Computer Applications* 28.2 (2011): 37-40.
24. Kannan, S., and Vairaprakash Gurusamy. "Preprocessing Techniques for Text Mining." ,ResearchGate, Conference Paper , October 2014
25. Sasaki, Yutaka. "Automatic text classification." University of Manchester: presentation (2008).
26. Khalid Hussain zargar , Manzoor Ahmad Chachoo, "Comparative Study Of Text Classification Methods", *International Journal For Technological Research In Engineering* ,Volume 2, Issue 8, April-2015
27. internet survey , sunny (2013) List of English stop words. Available at: <http://99webtools.com/blog/list-of-english-stop-words> (Accessed: 29 September 2016).
28. Chong, Man Yan Miranda. "A study on plagiarism detection and plagiarism direction identification using natural language processing techniques." (2013).
29. Tanya Taneja , Balraj Sharma , " Classification Using PSO & Other Technique ",*International Journal of Recent Development in Engineering and Technology*,Volume 3, Issue 1, July 2014
30. internet survey ,Classificationtable. Available at: <http://www.real-statistics.com/logisticregression/classification-table>
31. Chidiebere, Ugwu, and Obasi Chinedu Kingsley. "Legal Case Document Classification Application Based on an Improved Hybrid Approach." *International Journal of Engineering Research and Technology*. Vol. 4. No. 04 (April-2015). ESRSA Publications, 2015.
32. internet survey ,F1 score (2016) in Wikipedia. Available at: https://en.wikipedia.org/wiki/F1_score
33. internet survey, Revolvly, L. (no date) 'True positive rate' on Revolvly.Com. Available at: http://www.revolvly.com/main/index.php?s=True%20positive%20rate&item_type=top