GU J Sci, Part C, 6(2): 436-450 (2018)

Gazi Üniversitesi

Fen Bilimleri Dergisi

PART C: TASARIM VE TEKNOLOJİ

dergipark.gov.tr/http-gujsc-gazi-edu-tr

Spam SMS'lerin filtrelenmesinde yeni bir yaklaşım: Motif örüntüler

Yılmaz Kaya[1], Cüneyt Özdemir[2]

[1]*Siirt Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 00000, Merkez/SİİRT*

[2]*Siirt Üniversitesi, Teknik bilimler MYO*

Makale Bilgisi

Başvuru: 30/12/2017
Düzeltme: 14/02/2018
Kabul: 10/04/2018

Anahtar Kelimeler

SMS
Motif Örüntüler
Spam Filtreleme,
Metin Madenciliği

Keywords

SMSM
Motif Pattern
Spam Filtering
Text Mining

Öz

Her teknolojinin yaygınlaşması ile birlikte birçok problemde beraberinde gelir. Mobil teknolojilerde yaygın olarak kullanılan Mobil Kısa Mesaj Servisi(SMS) birçok sorunu beraberinde getirmiştir. SMS'in en önemli sorunu spam olarak belirtilen istenmeyen mesajların mobil ağ üzerinde yayılmasıdır. Spam mesajlar mobil trafiğini engellemekle birlikte kişileri de gereksiz yere meşgul etmektedir. Bu çalışmada spam SMS'leri filtrelemek için, karakterlerin UTF-8 kodlarını birbiri ile karşılaştırılması sonucu oluşan formları kullanan yeni bir öznitelik çıkarım, motif örüntüler yöntemi önerilmiştir. Önerilen motif örüntüler yönteminde, SMS'in unikodları üzerinde tanımlanan bir pencere boyutu (PB) içerisine giren değerlerin birbirlerine göre oluşturdukları formlar motif olarak ele alınmaktadır. SMS'deki bu motiflerin frekansları öznitelik vektörü olarak kullanılmıştır. Motif çeşitleri belirtilen PB'a bağlıdır. Motif örüntüler yöntemini test etmek için üç kıyaslama veri kümesi kullanılmıştır. Üç veri seti için sırası ile %93,76, %90.07 ve %94,29 başarı oranları gözlenmiştir. Gözlenen sonuçlara göre önerilen yöntemin spam filtrelenmesinde SMS mesajlarından başarılı öznitelik çıkarım yöntemi olduğu görülmüştür. Ayrıca motif yöntemi diğer metin madenciliği, doğal dil işleme alanlarında kullanılabileceği düşünülmektedir

A new approach to filtering spam SMS: Motif Patterns

Abstract

Along with the widespread of every technology, it comes with many problems. Mobile Short Message Service (SMS), which is widely used in mobile technologies, has brought many problems. The most important problem of SMS is unwanted messages named spam that are spread on the mobile network. Spam messages prevent mobile traffic and keep people busy unnecessarily. In this study to filter SMS spam, a novel feature extraction method, motif pattern method, is proposed, which uses forms that composed of comparision on UTF-8 codes of characters. In the proposed motif pattern method, the appearance of the values entered into a window size (PB) defined on the unicodes of SMS is considered as a motif pattern. The frequencies of these motifs in the SMS are used as the feature vector. The motif types depend on the specified PB. Three benchmark datasets were used to test the motif pattern method. The success rate was 93.76%, 90.07% and 94.29%, respectively, for three sets of data. According to the observed results, it is seen that the proposed method is a successful feature extraction method from SMS messages in spam filtering. It is also thought that the motif method can be used in other text mining, natural language processing fields.

1. GİRİŞ (INTRODUCTION)

Mobil teknolojilerinin en çok kullanılan hizmetlerinden ikisi kısa mesaj servisi (SMS) ve multimedya mesajlaşma (MMS) servisleridir [1]. Mobil üzerinden yapılan mesajlaşmalarda (SMS) görülen en önemli sorunlardan biri istenilmeyen mesajların (spam SMS) yayılmasıdır [1]. Günlük hayatta mobil iletişimde yoğun olarak kullanılan SMS mesajlarının mobil trafiğini yoğun olarak meşgul etmektedir. Bununla birlikte spam SMS'lerin varlığı mobil kullanıcıları ve mobil trafiği üzerinde sorunlara sebep olmaktadır [2]. SMS mesajların bu kadar yoğun gönderilmesinin sebebi ilk olarak SMS paketlerin tüm mobil iletişim için küresel system (Group Special Mobile=GSM) operatörlerinde ucuz olması; ikincisi mobil kullanıcıların bilgisayar kullanıcılarına göre daha interaktif olması ve SMS ile bilgilerin paylaşılmasında e-posta iletişimine göre güvenilir bulunmasından kaynaklanmaktadır. İnsanlar normal SMS mesajlarından çok spam SMS mesajlar almaktadır [3]. Spam mesajların eposta mesajlarına göre insanlar üzerinde daha

*e-mail: yilmazkaya1977@gmail.com, cuneytozdemir33@gmail.com

DOI:10.29109/http-gujsc-gazi-edu-tr.372880

büyük etkiye sahiptir. Çünkü insanlar genellikle gelen tüm SMS mesajlarına bakarlar. Kullanıcılara gelen SMS mesajların spam SMS olup olmadığına karar vermeleri zaman kaybına neden olur. Spam ağırlık olarak para kazanma, yetişkin ürünleri pazarlama, kilo verme, ürün tanıtma şeklinde kendini göstermektedir [4,5,6]. Spam SMS'lerin tanınması, filtrelenmesi için yeni alanlar ve farklı yaklaşımlar söz konusudur. İstatistiksel ve makine öğrenmesi yöntemleri spam filtrelemek için kullanılmaktadır [4,7,8,9].

SMS mesajlarının filtrelenmesi için en önemli aşama öznitelik bilgi çıkarımıdır. Çıkarılan öznitelikler, mesajları spam olarak değerlendirmenin başarısını etkiler. Ancak eposta spamlara göre SMS spamları içerik olarak çok daha kısa olması, çoğu zaman kısaltmalardan oluşması uygun özniteliklerin çıkarılmasını zorlaştırmaktadır [10]. Bu yüzden içeriğe göre uygun özniteliklerin elde edilmesi zor olmaktadır [11].

Bu çalışmada spam SMS mesajları filtrelemek için yeni bir öznitelik çıkarım metodu önerilmiştir. Önerilen yöntem, motif örüntüler yaklaşımı, karakterlerin birbirlerine göre oluşturdukları görünümlere dayanmaktadır. Motif yönteminin en önemli avantajı hesaplama basitliğidir. Bu yöntem gerçek zamanlı metin işleme uygulamalarında kullanılabilir. Önerilen yöntemde karakterlerin Unikod değerleri kullanılarak her karakterin etrafındaki komşu karakterlerin Unikod değerlerinin birbirleri ile karşılaştırmalar sonucunda oluşan örüntülere dayanmaktadır.

Motif desenler yöntemi sinyal üzerinde tanımlanan bir pencere içindeki değerlerin birbirlerine göre oluşturdukları büyüklük durumlara göre motif denilen formların frekanslarına bağlıdır. Örneğin pencere boyutu (PB) 4 seçildiğinde pencere içinde 4 adet değer (P1,P2,P3,P4) olacaktır. Bu değerlerin büyüklük değerlerine göre bir motif M1=P1>P2>P3>P4 şeklinde olabilir. Diğer bir motif P1>P3>P4>P2 şeklinde olabilir. Pencere içindeki değerlerin büyüklük değerlerine göre birbirlerine göre PB! adet motif elde edilir. Örneğin PB=4 olması durumunda 4!=24 adet motif, PB=5 olması durumunda 5!=120 motif bulunur. Farklı mikro-makro örüntülerin elde edilmesi için PB parametresi önemli olmaktadır. Önerilen yöntemi test etmek için üç farklı gerçek kıyaslama verisi kullanılmıştır. Motif örüntüler kullanılarak farklı sınıflandırma metotları ile 10 kat çapraz geçerlilik yöntemine göre sınıflandırma işlemleri gerçekleştirilmiştir.

2.LİTERATÜR BİLDİRİŞLERİ (LITERATURE NOTIFICATIONS)

Spam hem internet hem de mobil iletişimde önemli bir problemdir. Spam e-postaların filtrelenmesinde önemli çalışmalar yapılmıştır. Farklı spam engelleme metotları geliştirilmiştir. Makine öğrenmesi tabanlı yöntemler [12,13], özellik çıkarım yöntemleri fazlası ile kullanılmıştır. Bu yöntemler ile önemli başarılar sağlanmıştır. Ancak bu yöntemler SMS spamların engellenmesinde aynı başarıyı gösteremeyebilir. Çünkü SMS mesajları normal e-postalara göre hem çok kısa hem de kaynağı sürekli değişim gösterebilmektedir. Standart bir SMS mesajı uzunluğu 160 karakterdir. İçerik olarak eposta mesajlara göre SMS mesajlar çok fazla bilgi sağlamazlar. Çünkü insanlar SMS mesajı yazdıklarında standart olmayan yazılımlar geliştirirler. Örneğin "How are you" yerine "How r u" gibi yazılışlar geliştirebilirler [14]. SMS mesajların filtrelenmesine yönelik literatürdeki çalışmalar Delany ve arkadaşlarının [5] çalışmalarında verilmiştir. SMS spam filtrelemek için kara listeler ve içerik tabanlı modellerin kullanıldığı görülmektedir [15]. Kara listeler SMS mesajı gönderen kişilere ait telefon numaralarını veya anahtar kelimeleri saklayarak kimlerin spam gönderdiklerini tutarlar. Bu telefon numaralarından gelen mesajlar kara listedeki numaralar veya anahtar kelimeler ile karşılaştırılarak mesajlar spam klasörüne taşınır. Ancak bu yöntem her zaman istenilen başarıyı sağlamaz. Çünkü bu yöntem kara listedeki anahtar kelimelere bağlıdır. Bu anahtar kelimelerin yetersizliği, farklı yazılış şekilleri yüzünden spam olmayan mesajların bile engellenmesine neden olabilir. İçerik tabanlı yöntemler ise SMS mesajın içeriğine göre değerlendirme yapar. Mesajın içeriğindeki bazı anahtar kelimelerin aranması, kelime veya harf frekansları gibi mesaj içeriğini ele alan yöntemlerdir. Spam SMS'lerin filtrelenmesi için yapılan çalışmalara ait bir özet tablo aşağıda verilmiştir. Bu çalışmada önerdiğimiz motif örüntüler yöntemi hem SMS hem de e-posta spamların engellenmesinde kullanılabilir.

Tablo 1. *Spam SMS filtrelemek için yapılan çalışmalar*

Yazar/Yıl	Özellikler veya Sınıflandırıcı
Xiang, Chowdhury, ve Ali (2004) [21]	Karar destek vektörleri (SVM)
Healy, Delany, ve Zamolotskikh (2005) [22]	Knn
Cai, Tang, ve Hu (2008) [23]	Winnow Algoritması
Wu, Wu, ve Chen (2008) [24]	Bayes
Longzhen, An, ve Longjun (2009) [25]	Knn
Almeida, ve ark (2011) [26]	SVM, Knn, DT, C4.5i PART,
Deng ve Peng (2006) [27]	NB
Rafique ve Farooq (2010) [28]	HMM
Cormack ve ark. (2007) [29]	Bigrams öznitelikler
Sohn, Lee, ve Rim (2009) [30]	Biçimsel öznitelikler
He ve ark. (2008) [31]	Kara listeler
Healy ve ark. (2005) [23]	KNN, SVM, ve NB
Deng ve Peng (2006) [32]	SMS mesaj uzunluğu gibi karakteristik öznitelikler
Yoon ve ark. (2010) [1]	İçerik tabanlı filtreleme
Gómez Hidalgo ve ark. (2006) [33]	Sözcüksel öznitelikler, n-gram
Sohn ve ark. (2012) [34]	Sözcüksel ve sitil öznitelikler
Chen ve ark. (2015) [14]	Kelimelerin uzunluğuna dayalı özellikler
Ahmed ve ark. (2015) [35]	Apripri+NB
Ali ve ark. (2015) [36]	Dendritic Cell Algoritması
Adebukola ve ark. (2015) [37]	Yapay Bağışıklık Sistemi
Ho ve ark. (2013) [38]	Graf tabanlı Knn Algoritması
NK Nagwani (2017) [39]	NB, SVM, NMF, LDA
Zhang ve ark., (2016) [40]	Özel kelimeler+SVM,NB
Karasoy O., Ballı S., (2017) [41]	Word2Vec+RF,NB,MLP..
Pham ve ark.,(2016) [42]	Kelime Frekansı+BOW
Najadat ve ark. (2014) [43]	NB, Knn, RF, J48
Rafique ve Abulaish (2012, August). [44]	Kelime grafları
Rafique ve ark. (2011) [45]	Evrimsel algoritmalar
Almeida ve ark. (2016) [46]	Semantik indeksleme
Akbari, ve Sajedi (2015) [47]	En çok tekrar eden kelime frekansları
Kim ve ark. (2015) [48]	Anahtar kelime frekansları
Mahmoud ve Mahfouz (2012) [49]	Yapay bağışıklık sistemi
Mujtaba ve Yasin (2014). [50]	Harf frekansları, mesaj uzunlukları

3.VERİ SETLERİ (DATASETS)

Bu çalışmada 3 farklı gerçek kıyaslama veri seti kullanıldı. Bu veri setleri hem yaygın bir şekilde kullanılmalarından hem de kolay ulaşılabilir olmalarından dolayı tercih edilmiştir. Bu 3 veri setinin özellikleri aşağıda özetlenmiştir.

1- SMS Spam Veri Tabanı v.0.1 (Veri Seti 1, VS1): Bu veri seti SMS spam araştırmaları için oluşturulmuştur. Bu veri kümesinde 322 spam ve 1002 adet spam olmayan SMS mesajı bulunmaktadır. Birçok araştırmada kullanılan bu veri seti Cornack ve ark. [11] tarafından oluşturulmuştur. Veri kümesindeki ortalama kelime sayısı 15,72 ve kelimelerin ortalama uzunluğu 4.44 karakterdir.

2-British English SMS Veri Tabanı (Veri Seti 2, VS2). Veri seti GrumbleText web sayfasından elde edilmiştir [51]. GrumbleText web sitesi kullanıcıların spam SMS'leri şikayet amaçlı girdikleri bir sitedir. İnsanlar bir spam SMS aldıkları zaman gönüllü olarak bu siteye girerler. Bu veri seti 425 spam ve 450 spam olmayan mesaj içerir.

3- En son veri setimiz (Veri Seti 3, VS3) Almeida ve arkadaşları [9] tarafından oluşturulmuş SMS spam veri kümesidir. Veri kümesi 747 spam ve 4827 spam olmayan toplamda 5574 SMS mesajdan oluşmaktadır. Spam mesajlar tüm veri kümesinin %13,4'ünü oluşturmaktadır.

Önerilen metot ile ayırt edici özelliklerin yakalanması için SMS mesajların belirli uzunlukta olması gerekir. Çalışmada 30 karakterin altındaki mesajlar veri kümelerinden çıkarılmıştır. Geriye kalan SMS mesajların oranları Tablo 2'de gösterilmiştir.

Tablo 2. *Veri kümelerindeki mesajların dağılımı*

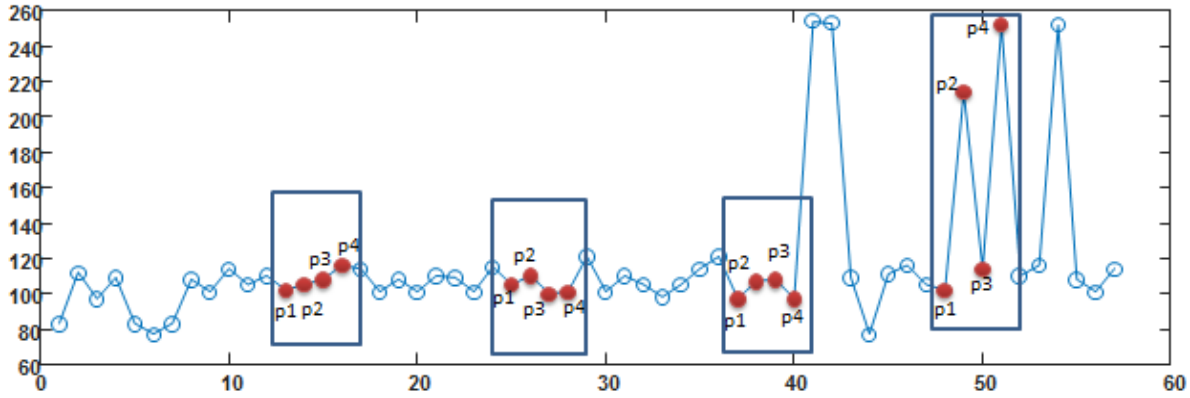
Veri Seti	#Spam mesaj	#Normal Mesaj	Toplam
VS1	321	592	913
VS2	419	367	786
VS3	740	3162	3902

4. METOT (METHOD)

4.1. Özellik Çıkarımı & Motif Örüntüler (Feature Extraction & Motif Patterns)

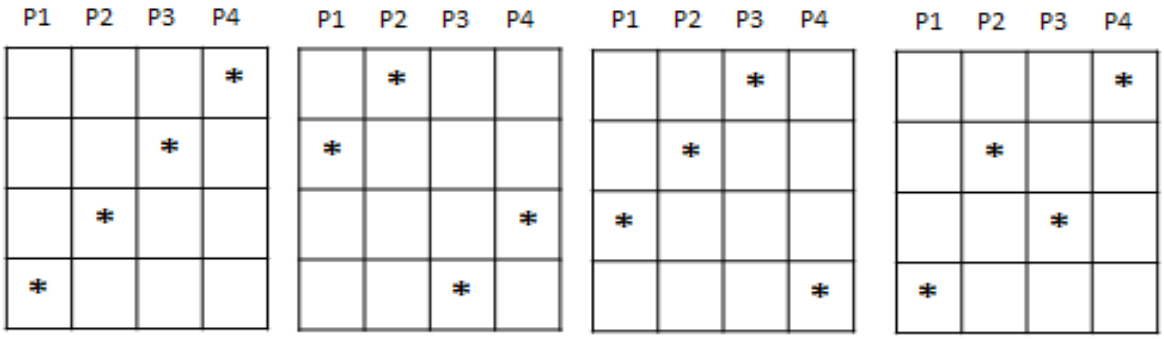
Motif örüntüler yöntemi, metin tabanlı SMS mesajlarından etkili öznitelikler çıkarmak için kullanılmıştır. Motif yöntemi, mesaj içindeki her karakterin UTF-8 değerlerin birbirleri ile karşılaştırılması sonucu elde edilen görünümleri kullanmaktadır. SMS mesajların unikod dizilerinden motif denilen yapıları çıkararak normal SMS'ler spam SMS'lerden ayrıştırılmıştır.

Motif örüntüler SMS içindeki karakterlere ait unikodların birbirlerine göre oluşturdukları yapılardır. Motif sayısı mesaj üzerindeki alınan komşu sayısına, diğer bir deyişle pencere boyutuna (PB) bağlıdır. PB= 3 olarak alındığında 3!=3*2*1=6, PB= 4 alındığında ise 4!=4*3*2*1=24 motif elde edilir. Motif örüntülerin elde ediliş şekli Şekil 2'deki işaret örneği üzerinde anlatılmıştır. Aşağıdaki işaretlerde PB=4 alınmıştır. Her pencere içinde 4 adet işaret değeri (P1,P2,P3 ve P4) bulunur. Bu değerlerin birbirlerine göre büyüklükleri bir motif olarak alınmaktadır.



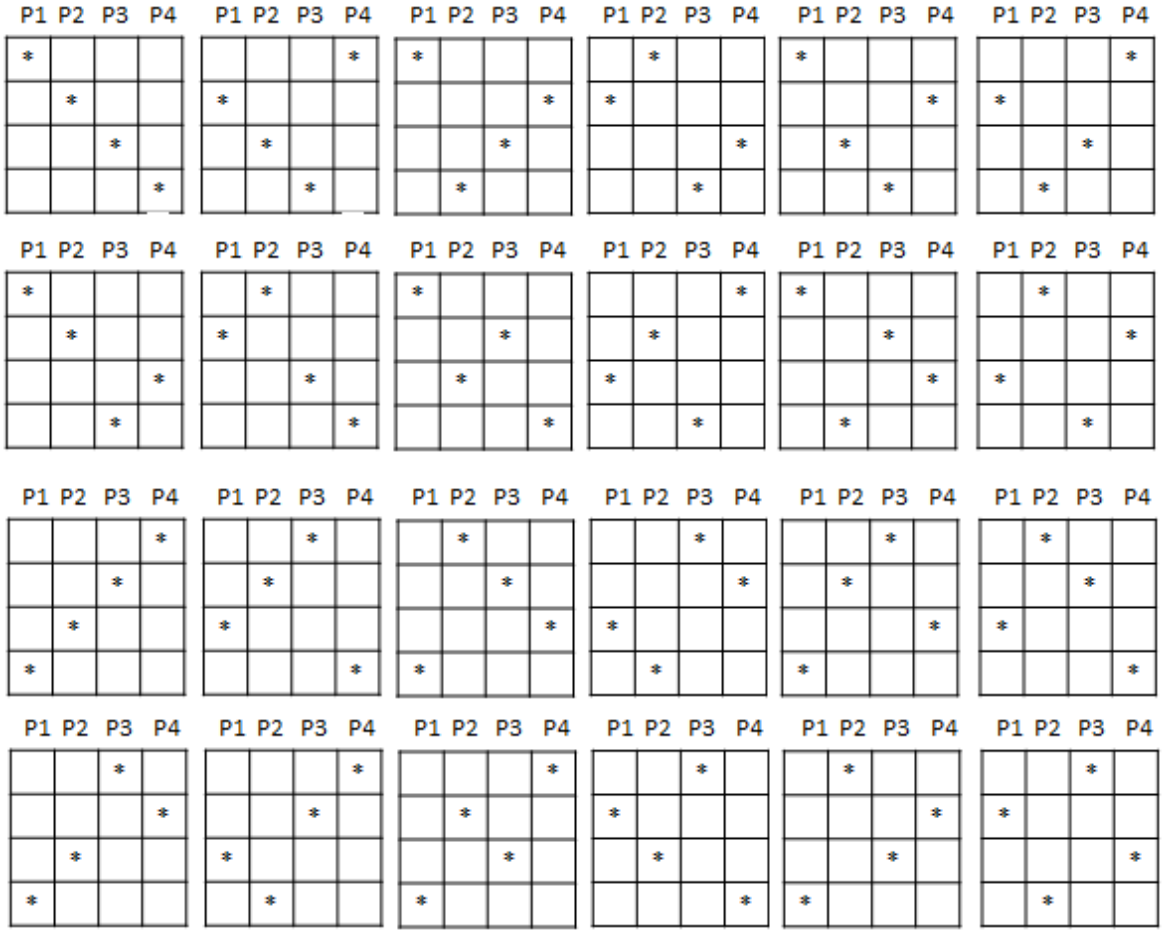
Şekil 2. *Örnek bir SMS için unikod değerlerin gösterilmesi*

Şekil 2'e bakıldığında 4 örnek pencere verilmiştir. Birinci penceredeki değerlerin oluşturduğu motif (P4>P3>P2>P1) şeklindedir. İkinci penceredeki motif (P2>P1>P4>P3), üçüncü penceredeki motif (P3>P2>P1>P4) ve son penceredeki motif ise (P4>P2>P3>P1) şeklindedir. Bu motifler Şekil 3'te verilmiştir.



Şekil 3. *Şekil 2'deki işaret üzerindeki örnek motifler*

Motif sayıları ve formları PB'na bağlıdır. Bu örnekte_PB=4 olarak alınmıştır. Dolayısıyla 24 adet motif örüntü elde edilmiştir. İşaret üzerindeki her motif örüntü frekansı bir öznitelik olarak alınır. PB=4 olması durumunda elde edilecek diğer motifler Şekil 4'te verilmiştir.



Şekil 4. *PB=4 olması durumunda oluşan motifler*

4.2. Performans Ölçütleri (Performance Measures)

Önerilen motif örüntüler yönteminin başarısını ölçmek için iyi bilinen aşağıdaki ölçütler kullanılmıştır [17].

Doğruluk oranı ölçütü: Doğru sınıflandırılmış örneklerin oranını belirtir.

Spam Caught (SC) ölçütü: Doğru sınıflandırılmış spam örneklerin oranıdır,

Blocked Hams (BH) : Doğru sınıflandırılmış non-spam SMS'lerin oranını belirtir.

Matthews Korelasyon Katsayısı (MKK): Bu ölçü netlik, hassasiyet ve F1-Score metriklerine bakılmaksızın iki sınıflandırma işlemlerinde en güvenilir sonucu veren performans ölçütüdür.

Bu ölçütler spam filtrelemek için kullanılan yöntemlerin değerlendirilmesinden yaygın bir şekilde kullanılmaktadır [17,18,19,20]. Bu ölçütler aşağıdaki gibi tanımlanır:

$$Doğruluk = \frac{N_{TP}+N_{TN}}{N_F+N_T} \quad (1)$$

$$SC = \frac{N_{TP}}{N_{TP}+N_{FP}} \quad (2)$$

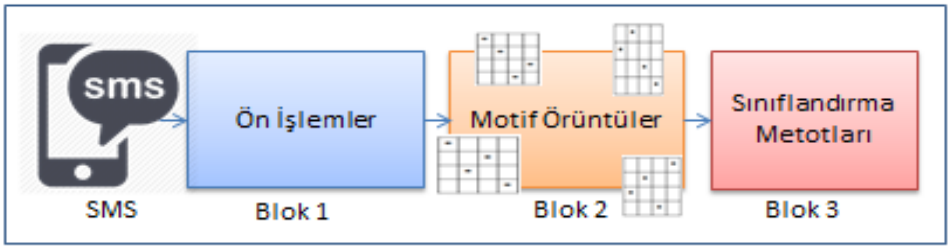
$$BH = \frac{N_{TN}}{N_{TN}+N_{FN}} \quad (3)$$

$$MKK = \frac{N_{TP}xN_{TN}-N_{FP}xN_{FN}}{\sqrt{(N_{TP}+N_{FP})(N_{TP}+N_{FN})(N_{TN}+N_{FP})(N_{TN}+N_{FN})}} \quad (4)$$

Burada N_T toplam spam SMS sayısı, N_F toplam spam olmayan SMS sayısı, N_{TP} toplam doğru sınıflandırılmış spam SMS sayısı, N_{FP} toplam non-spam SMS ancak spam olarak sınıflandırılmış SMS sayısını ve N_{FN} ise toplam spam SMS olup ancak non-spam olarak sınıflandırılmış SMS sayısını ifade eder.

4.3. Spam Filtreleme Aşamaları (Spam Filtering Phases)

Bu makalede spam olan SMS'lerifiltrelemek için yeni bir öznitelik çıkarım yöntemi önerilmiştir. Önerilen motif yöntemi karakterlerin büyüklük olarak birbirleri ile oluşturdukları görünümlere dayanan istatistiksel bir yaklaşımdır. Spam filtreleme aşamaları aşağıdaki blok diyagramda gösterilmiştir.



Şekil 5. *Spam filtreleme blok diyagramı*

Blok 1: Bu bölümde SMS mesajı içindeki noktalama işaretleri, boşluk, satır başı, satır sonu gibi özel karakterler temizlenir. Geriye kalan kısım Unikodlara dönüştürülür. Unikodları elde edilen SMS tek boyutlu vektör olarak düşünülür. Örneğin aşağıdaki SMS mesajı için bu işlemi gerçekleştirdiğimizde;

"Spam SMS'lerin filtrelenmesinde yeni bir yaklaşım: Motif Örüntüler"

İlk önce istenmeyen gereksiz karakterlerin atılması gerekir. Gereksiz karakterler atıldıktan sonra yeni mesaj:

"*SpamSMSlerinfiltrelenmesindeyenibiryaklaşımMotifÖrüntüler*"

olarak elde edilir. Yeni oluşan mesaj UTF-kodlarına dönüştürülür. Bu kodlar;

"83 112 97 109 83 77 83 108 101 114 105 110 102
105 108 116 114 101 108 101 110 109 101 115 105
110 100 101 121 101 110 105 98 105 114 121 97
107 108 97 254 253 109 77 111 116 105 102 214
114 252 110 116 252 108 101 114"

şeklinde elde edilir.

Block 2: Bu bölümde önişlem aşamasından geçen SMS'lerden motif örüntüler yöntemi ile öznitelikler çıkarılmaktadır. Elde edilen öznitelik vektörü boyutu sinyal üzerinde tanımlanan PB'na bağlıdır. PB'nin büyümesi maliyeti artırmaktadır. Ancak daha ayırt edici özniteliklerin elde edilmesini sağlar. PB parametresi SMS mesajlarında farklı örüntülerin aranması için önemli olmaktadır.

Block 3: Sınıflandırılma aşamasıdır. Bu bölümde Tek bağımlılık tahminleyici (Aggregating One-Dependence Estimators= A1DE), Yapay sinir ağları (Artificial Neural Network=ANN), Destek vektör makinası(Support Vector Machine=SVM), lojistik regresyon (Logistic Regression=LR), Fonksiyonel Ağaç (Functional Tree=FT) ve Rastgele orman Random Forest=RF) gibi farklı makine öğrenmesi yöntemler kullanılmıştır. Motif örüntüleri kullanarak makine öğrenmesi yöntemler ile SMS'ler spam veya non-spam şeklinde sınıflandırılmıştır.

5. SONUÇLAR (RESULTS)

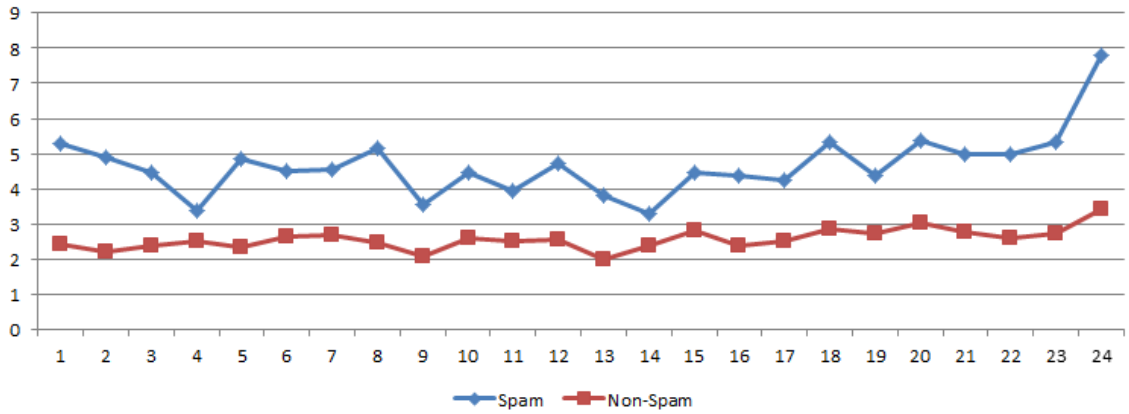
5.1. Motif Örüntüler (Motif Pattern)

Bu makalede spam SMS'lerin filtrelenmesi için karakterlerin UTF-8 değerlerini kullanan yeni bir özellik çıkarım Motif örüntüler yöntemi önerilmiştir. Bu yöntem ile SMS mesajların non-spam ve spam olarak sınıflandırılması için SMS'lerden öznitelikler elde edilmiştir. Önerilen yöntemin en güçlü özelliği serideki en küçük değişimlerine hassasiyet ve hesaplama kolaylığıdır. PB parametresi, SMS mesajlarındaki farklı baskın öznitelikleri elde edebilmek için farklı ölçeklerde kullanılabilir. Bu çalışmada 3 farklı veri seti kullanıldı. PB=4 olması durumunda VS1 veri kümesinden elde edilen motiflere ait ortalama ve standart sapma (SS) değerleri Tablo 3'te verilmiştir. Elde edilen motif ortalamaları Şekil 6'dan görülebilir. Tabloya bakıldığında motif ortalamaların spam ve non-spam örnekler için farklı olduğu görülmektedir.

Tablo 3*. VS1 için PB=4 olması durumunda elde edilen motiflere ait ort. ve SS'lar*

Motif	**Non-Spam**		**Spam**	
	Ortalama	**S. Sapma**	**Ortalama**	**S. Sapma**
M1	2,41	2,12	5,26	2,62
M2	2,19	1,60	4,90	2,14
M3	2,38	1,73	4,47	2,01
M4	2,52	1,85	3,39	1,88
M5	2,33	1,70	4,85	2,18
M6	2,65	1,97	4,51	2,09
M7	2,67	1,79	2,56	1,92
M8	2,46	1,85	5,13	2,25
M9	2,07	1,56	3,55	1,91
M10	2,59	1,91	4,45	2,21
M11	2,52	2,04	3,93	2,06
M12	2,55	1,84	4,73	2,17
M13	1,99	1,57	3,80	1,83
M14	2,40	1,81	3,28	1,85
M15	2,83	1,97	4,47	2,12
M16	2,39	1,74	4,39	1,96
M17	2,50	1,93	4,25	2,02
M18	2,87	1,89	5,33	2,11

M19	2,72	1,98	4,36	2,11
M20	3,01	2,11	5,37	2,09
M21	2,77	1,82	4,99	2,20
M22	2,61	1,89	4,97	2,26
M23	2,71	1,81	5,31	2,00
M24	3,43	2,59	7,80	3,64



***Şekil 6**. PB=4 olması durumunda spam ve non-spam SMS mesajlar için elde edilen motif ortalamaları*

Şekil 6'ya bakıldığında spam ve non-spam SMS'lerden elde edilen motif örüntülerin sayısının farklı sayıda olduğu görülmektedir. SMS'lerde PB'ye göre motiflerin sayının spam ve non-spam sınıflar için farklı sayıda olması başarı oranını yükseltecektir.

5.2. Sınıflandırma Sonuçları (Classification Results)

Motif analizi farklı PB değerlerinin kullanılması ile gerçekleştirilebilir. PB parametresinin büyük değerleri hem öznitelik uzayını büyütür. Bununda yanında sınıflandırma sürecinde işlem maliyetini artırır. PB'nin küçük değerleri ise etkin özniteliklerin elde edilmesini engelleyebilir. Bilgi kaybına neden olabilmektedir. Uygun PB değerlerine denemeler sonucunda karar verilmelidir. PB'nin farklı değerleri için elde edilen motif örüntüler kullanılarak gözlenen sınıflandırma başarı oranları Tablo 4-6'da verilmiştir. Açık kaynak kodlu bir yazılım olan WEKA kullanılarak sınıflandırma işlemleri gerçekleştirilmiştir [18].

***Tablo 4**. VS1 için başarı sonuçları (%)*

PB	**#Öznitelik**	**RF**	**SVM**	**ANN**	**LR**	**FT**	**A1DE**
4	24	88.28	85.65	87.84	87.62	87.40	85.76
5	120	91.23	90.47	88.17	85.98	87.51	87.51
6	720	92.99	92.22	91.56	92.77	90.91	92.00
7	5040	91.02	90.58	93.10	**93.76**	91.45	91.77

Tablo 4'teki başarı oranlarından görüldüğü gibi PB parametresi ile farklı örüntülerin elde edildiği anlaşılmaktadır. VS1 veri kümesi için en yüksek başarı oranı PB=7 olması durumunda elde edile motifler kullanılarak elde edilmiştir. Başarı oranı %93.76 olarak gözlenmiştir. Elde edilen başarı oranları kabul

edilebilir önemli sonuçlardır. En yüksek başarı oranı LR ile gözlenmiştir. Ancak genel olarak en başarılı sınıflandırıcı RF yöntemi olarak gözlenmiştir. Diğer makine öğrenmesi yöntemler ile de yüksek başarılı sonuçların elde edildiği görülmektedir.

Tablo 5*. VS2 için başarı sonuçları (%)*

PB	#Öznitelik	RF	SVM	ANN	LR	FT	A1DE
4	24	84.60	82.70	81.68	84.10	80.28	82.18
5	120	86.77	84.73	82.18	82.82	82.95	88.29
6	720	88.17	88.42	86.64	87.40	83.33	88.29
7	5040	88.16	83.84	88.80	**90.07**	86.51	88.04

VS2 için en yüksek başarı oranı P=7 olması durumunda elde edilen öznitelikler ile LR kullanılarak elde edilmiştir. Gözlenen başarı oranı %90,07'dir. Kullanılan sınıflandırma yöntemleri arasında en yüksek başarıyı genel olarak A1DE göstermiştir.

Tablo 6*. VS3 için başarı sonuçları*

PB	#Öznitelik	RF	SVM	ANN	LR	FT	A1DE
4	24	91.85	81.03	90.15	87.00	88.69	85.75
5	120	93.05	86.62	91.85	91.33	90.79	88.67
6	720	92.26	82.21	92.26	90.08	94.05	91.23
7	5040	**94.29**	91.90	94.15	93.92	93.66	93.25

Son veri seti VS3 için en yüksek başarı %94,29 olarak elde edilmiştir. Bu başarı PB=7 olduğunda elde edile öznitelikleri kullanarak RF ile gözlenmiştir. Sonuç olarak tüm veri setleri için elde edilen sonuçlar kabul edilebilir önemli sonuçlardır. PB boyutu arttıkça başarının arttığı görülmektedir. PB'nin yüksek değerleri için farklı ayırt edici motiflerin elde edildiği anlaşılmaktadır. Çünkü PB'nin boyutuna göre çıkarılan motif sayısı ciddi anlamda artmaktadır. Bu da farklı mikro-makro motiflerin elde edilmesini sağlamaktadır. En yüksek başarıyı sağlayan öznitelikler ve makine öğrenmesi yöntemlerin SC, BH, başarı ve MKK performans değerleri Tablo 7'de verilmiştir.

Tablo 7*. Üç veri seti için performans ölçütleri*

Özellikler / Sınıflandırıcı	Veriseti	SC(%)	BH(%)	Başarı(%)	MKK
(PB=7)+LR	VS1	90.15	95.66	93.76	0.87
(PB=7)+LR	VS2	90.21	89.91	90.07	0.80
(PB=7)+RF	VS3	84.32	98.79	94.29	0.81

Tabloya bakıldığında sonuçların önemli olduğu görülmektedir. BH ve MKK değerleri spam olmayan SMS'lerin spam SMS'lerden ayrışmalarının önemini belirtir. Tüm veri setleri için BH değerin yüksek olduğu görülmektedir. Non-Spam bir SMS'in spam olarak değerlendirilmesi, spam olan bir SMS'in non-spam olarak değerlendirilmesinden daha önemlidir. Çünkü non-spam olan önemli bir SMS'in spam olarak değerlendirilmesi durumunda görülmeme riski mevcuttur. MKK ve BH ölçütleri filtrelenen spam

SMS sayısı ile spam olarak ele alınan non-spam SMS'ler arasındaki dengeyi ölçerler. SC ölçütü spam SMS'leri filtrelenme başarısını ifade eder. VS1 ve VS2 veri setleri için daha başarılı sonuçlar gözlenmiştir.

Önerilen yöntemin güçlülüğünü test etmek için veri setleri arasında eğitim-test setleri şeklinde çaprazlama yapıldı. Örneğin VS1 veri kümesini eğitim, VS2 ve VS3 veri kümelerini test setleri olarak ele alındı. Diğer çaprazlamalar ve gözlenen başarı oranları Tablo 8'de verilmiştir. Sınıflandırma işlemleri RF ile gerçekleştirildi.

Tablo 8. *Çaprazlama Sonuçları*

PB	**Eğitim-Test**	**Başarı (%)**	**Eğitim- Test**	**Başarı (%)**
4	VS1–VS2	82.69	VS1-VS3	85.82
4	VS2-VS1	84.77	VS2-VS3	81.90
4	VS3–VS1	98.80	VS3-VS2	100.00
5	VS1-VS2	82.82	VS1-VS3	89.69
5	VS2-VS1	86.19	VS2-VS3	82.95
5	VS3-VS1	99.23	VS3-VS2	100.00
6	VS1-VS2	88.11	VS1-VS3	92.67
6	VS2-VS1	91.01	VS2-VS3	88.98
6	VS3-VS1	99.45	VS3-VS2	100.00

Tablo 8'e bakıldığında %82.69 ile %100 arasında başarı oranları gözlenmiştir. Düşük başarı oranları eğitim veri setindeki (VS1=913, VS2=786) SMS'lerin sayısının azlığından ve test setindeki (VS3=3902) SMS'lerin fazla olmasından kaynaklanmıştır. Tam tersi yüksek başarı oranları eğitim veri setindeki (VS3) SMS'lerin fazla ve test setlerindeki (VS1, VS2) SMS'lerin sayısının az olmasından kaynaklanmıştır. VS3 veri setinin eğitim seti olarak kullanılması durumunda VS1 veri seti için %99.45 ve VS2 veri seti için %100 başarı gözlenmiştir.

6. TARTIŞMA ve SONUÇ (DISCUSSION & RESULTS)

Mobil ağlar verilerin paylaşılmasında, sosyal ağların geliştirilmesinde modern hayatın vazgeçilmezi durumuna gelmiştir. Gelişen mobil teknolojileriyle birlikte iletişimin en önemli araçlarından biri mobil SMS'ler olmuştur. SMS mesajların yaygınlaşması ile bu hizmeti kötü amaçları için kullanmak isteyen kişi veya şirketlerin odağı haline getirmiştir.. Günlük hayatta sıkça kullandığımız SMS mesajlaşmalarda görülen spam sms'lerin çokluğu, mobil trafiği ve kullanıcıları için bir problem haline gelmiştir. Bu çalışma kapsamında spam SMS'leri filtrelemek için, yeni bir öznitelik çıkarım yöntemi olan motif örüntüler önerilmiştir. Bu metota göre mesajlar unikoda dönüştürülür ve her değer komşuları ile yeni görünümler oluşturur. Motif yönteminin en önemli avantajı hesaplama basitliğidir. Bu yöntem gerçek zamanlı metin işleme uygulamalarında kullanılabilir. Ayrıca motif yöntemde kullanılan PB parametresi ile farklı mikro-makro motifler elde edilebilir. PB arttıkça elde edilen motif sayısı faktöriyel artış göstermektedir. PB'nin büyük değerleri için motif sayısı artacaktır. Bu da sınıflandırma metotları için hesaplama maliyetini artırmaktadır. Bu çalışmada PB=7 olarak ayırtedici motifler elde edilmiştir. Motif örüntüler metodunu test etmek için 3 farklı kıyaslama veri kümesi kullanılmıştır. Üç farklı veri kümesi için sırasıyla %93.76, %90.07 ve %94.29 gibi kabul edilebilir başarı oranları gözlenmiştir. Sonuç olarak gözlenen sonuçlara göre motif örüntüler yöntemi metin SMS mesajlarından öznitelik çıkarımı için önemli örüntüler sağladığı görülmüştür. Bu özellik çıkarım yönteminin diğer doğal dil işleme ile ilgili çalışmalarda kullanılabileceği düşünülmektedir.

KAYNAKÇA (REFERENCES)

[1] Ji Won Yoon, Hyoungshick Kim, Jun Ho Huh, 2010, Hybrid spam filtering for mobile communication, computers & security 29 (2010) 446–459.

[2] Chen, L., Yan, Z., Zhang, W., & Kantola, R. (2014). TruSMS: A trustworthy SMS spam control system based on trust management. Future Generation Computer Systems. http://dx.doi.org/10.1016/j.future.2014.06.010

[3] Ahmed, I, Ali, R, Guan, D, Lee, YK, Lee, S, Chung, TSemi-supervised learning using frequent itemset and ensemble learning for SMS classification. Expert Systems with Applications, 2015, 42(3): 1065–1073.

[4] Su, MC, Lo, HH, Hsu, FH, A neural tree ve its application to spam e-mail detection. Expert Systems with Applications, 37(12), 2010, 7976-7985.

[5] Delany, S. J., Buckley, M., & Greene, D. (2012). SMS spam filtering: methods ve data. Expert Systems with Applications, 39(10), 9899-9908.

[6] A. K. Uysal, S. Gunal1, S. Ergin, E. Sora Gunal, 2013. The Impact of Feature Extraction ve Selection on SMS Spam Filtering, ELEKTRONIKA IR ELEKTROTECHNIKA, ISSN 1392-1215, VOL. 19, NO. 5, 2013

[7] Healy M, Delany S, Zamolotskikh A. An assessment of case-based reasoning for short text message classification. In: Proceedings of 16th Irish conference on artificial intelligence ve cognitive science; 2005. p. 257–66.

[8] Idris, I, Selamat, A, Omatu, S, Hybrid email spam detection model with negative selection algorithm ve differential evolution. Engineering Applications of Artificial Intelligence, 2014, 28, 97-110.

[9] Almeida, T. A., Gomez Hidalgo, J. M., & Yamakami, A. (2011). In Proceedings of the 11th ACM Symposium on document engineering DOCENG'11 (pp. 259-262). Mountain View, CA, USA: ACM.

[10] Wuying Liu, Ting Wang, 2010, Index-based Online Text Classification for SMS Spam Filtering, JOURNAL OF COMPUTERS, VOL. 5, NO. 6, JUNE 2010

[11] Cormack, G.V., Lynam, T.R., 2007. Online supervised spam filter evaluation. ACM Trans. Inform. Syst. 25 (3), 1–31.

[12] Y.-T. Hou, Y. Chang, T. Chen, C.-S. Laih, C.-M. Chen, Malicious web content detection by machine learning, Expert Syst. Appl. 37 (1) (2010) 55–60

[13] A.H. Wang, Detecting spam bots in online social networking sites: a machine learning approach, in: Data ve Applications Security ve Privace

[14] Liang Chen, Zheng Yan, Weidong Zhang, Raimo Kantola, 2015, TruSMS: A trustworthy SMS spam control system based on trust management. Future Generation Computer Systems 49 , 77-93

[15] M. Tufiq, M.F.A. Abdullah, K. Kang, D. Choi, A survey of preventing, blocking ve filtering Short Message Services (SMS) spam, in: Proc. of International Conference on Computer ve Electrical Engineering. IACSIT, November 2010, Vol. 1, pp. 462–466

[16] T. A. Almeida, A. Yamakami, ve J. Almeida. Evaluation of Approaches for Dimensionality Reduction Applied with Naive Bayes Anti-Spam Filters. In Proc. of the 8th IEEE ICMLA, pages 517–522, Miami, FL, USA, 2009.

[17] I. H. Witten ve E. Frank, Data Mining: Practical Machine Learning Tools ve Techniques, 2nd ed. San Francisco, CA: Morgan Kaufmann, 2005.

[18] Biggio, B., Fumera, G., Pillai, I., Roli, F. (2011). A survey ve experimental evaluation of image spam filtering techniques. Pattern Recognition Letters,32(10), 1436-1446.

[19] Laorden, C., Ugarte-Pedrero, X., Santos, I., Sanz, B., Nieves, J., Bringas, P. G. (2014). Study on the effectiveness of anomaly detection for spam filtering.Information Sciences, 277, 421-444.

[20] Sakkis, G., Veroutsopoulos, I., Paliouras, G., Karkaletsis, V., Spyropoulos, C. D., Stamatopoulos, P. (2003). A memory-based approach to anti-spam filtering for mailing lists. Information Retrieval, 6(1), 49-73.

[21] Xiang, Y., Chowdhury, M., & Ali, S. (2004). Filtering mobile spam by support vector machine. In N. Debnath (Ed.),Proceedings of the third international conference on computer sciences, software engineering, information technology, E-business ve applications(pp. 1–4)

[22] Healy, M., Delany, S., & Zamolotskikh, A. (2005). An assessment of case-based reasoning for short text message classification. In N. Creaney (Ed.),Proceedings of 16th Irish conference on artificial intelligence ve cognitive science, (AICS-05) (pp. 257–266)

[23] Cai, J., Tang, Y., & Hu, R. (2008). Spam filter for short messages using winnow. In Proceedings of the international conference on advanced language processing ve web information technology(pp. 454–459). IEEE

[24] Wu, N., Wu, M., & Chen, S. (2008). Real-time monitoring ve filtering system for mobile SMS. InProceedings of 3rd IEEE conference on industrial electronics ve applications(pp. 1319–1324)

[25] Longzhen, D., An, L., & Longjun, H. (2009). A new spam short message classification. In Proceedings of the first international workshop on education technology ve computer science(Vol. 2, pp. 168 –171).

[26] Almeida, T. A., Gómez Hidalgo, J. M., & Yamakami, A. (2011). InProceedings of the 11th ACM Symposium on document engineering DOCENG'11 (pp. 259-262). Mountain View, CA, USA: ACM.

[27] Deng, W.-W., & Peng, H., 2006. Research on a Naive Bayesian Based Short Message Filtering System. In Proceedings of the international conference on machinelearning ve cybernetics (pp. 1233–1237). IEEE.

[28] Rafique, M. Z., & Farooq, M. (2010). SMS SPAM detection by operating on byte-level distributions using hidden markov models (HMMs). InProceedings of the 20th virus bulletin international conference.

[29] G. V. Cormack, J. M. Gómez Hidalgo, ve E. Puertas Sanz, "Feature Engineering for Mobile (SMS) Spam Filtering," in Proceedings of the 30th Annual International ACM SIGIR Conference on Research ve Development in Information Retrieval, New York, NY, USA, 2007, pp. 871–872.

[30] Sohn, D. N., Lee, J. T., & Rim, H. C. (2009). The contribution of stylistic information to content-based mobile spam filtering. In Proceedings of the ACL/AFNLP 2009 conference short papers(pp. 321–324).

[31] He P, Sun Y, Zheng W, Wen X. Filtering short message spam of group sending using CAPTCHA. In: Workshop on knowledge discovery ve data mining; 2008. p. 558–61.

[32] Deng W, Peng H. Research on a naive Bayesian based short message filtering system. In: Machine learning ve cybernetics, 2006 international conference on Aug. 2006. p. 1233–7.

[33] J. M. Gómez Hidalgo, G. Cajigas Bringas, E. Puertas Sanz, ve F. Carrero García, "Content Based SMS Spam Filtering," in Proceedings of the 2006 ACM Symposium on Document Engineering, Amsterdam, The Netherlves, 2006, pp. 107–114.

[34] Dae-Neung Sohn, Jung-Tae Lee, Kyoung-Soo Han, Hae-Chang Rim, 2012, Content-based mobile spam classification using stylistically motivated features, Pattern Recognition Letters 33 (2012) 364–369

[35] Ishtiaq Ahmed, Rahman Ali, Donghai Guan, Young-Koo Lee, Sungyoung Lee, TaeChoong Chung, 2015. Semi-supervised learning using frequent itemset ve ensemble learning for SMS classification, Expert Systems with Applications 42 (2015) 1065–1073

[36] Ali A. Al-Hasan, El-Sayed M. El-Alfy, 2015, Dendritic Cell Algorithm for Mobile Phone Spam Filtering, Procedia Computer Science 52 (2015) 244 – 251

[37] Adebukola S. Onashoga, Olusola O. Abayomi-Alli, Adesina S. Sodiya & David A. Ojo, 2015, Information Security Journal: A Global Perspective, Information Security Journal: A Global Perspective, 00:1–13, 2015

[38] Tran Phuc Ho, Ho-Seok Kang, Sung-Ryul Kim, Graph-based KNN Algorithm for Spam SMS Detection, Journal of Universal Computer Science, vol. 19, no. 16 (2013), 2404-2419

[39] Nagwani, N. K. (2017). A Bi-Level Text Classification Approach for SMS Spam Filtering ve Identifying Priority Messages. International Arab Journal of Information Technology (IAJIT), 14(4).

[40] Zhang, X., Xiong, G., Hu, Y., Zhu, F., Dong, X., & Nyberg, T. R. (2016, June). A method of SMS spam filtering based on AdaBoost algorithm. In Intelligent Control ve Automation (WCICA), 2016 12th World Congress on (pp. 2328-2332). IEEE.

[41] Karasoy, O., & Ballı, S. (2017, October). Classification Turkish SMS with deep learning tool Word2Vec. In Computer Science ve Engineering (UBMK), 2017 International Conference on (pp. 294-297). IEEE.

[42] Pham, T. H., & Le-Hong, P. (2016, November). Content-based approach for Vietnamese spam SMS filtering. In Asian Language Processing (IALP), 2016 International Conference on (pp. 41-44). IEEE.

[43] Najadat, H., Abdulla, N., Abooraig, R., & Nawasrah, S. (2014). Mobile sms spam filtering based on mixing classifiers. International Journal of Advanced Computing Research, 1, 1-7.

[44] Rafique, M. Z., & Abulaish, M. (2012, August). Graph-based learning model for detection of SMS spam on smart phones. In Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International (pp. 1046-1051). IEEE.

[45] Rafique, M. Z., Alrayes, N., & Khan, M. K. (2011, July). Application of evolutionary algorithms in detecting SMS spam at access layer. In Proceedings of the 13th annual conference on Genetic and evolutionary computation (pp. 1787-1794). ACM.

[46] Almeida, T. A., Silva, T. P., Santos, I., & Hidalgo, J. M. G. (2016). Text normalization and semantic indexing to enhance Instant Messaging and SMS spam filtering. Knowledge-Based Systems, 108, 25-32.

[47] Akbari, F., & Sajedi, H. (2015, May). SMS spam detection using selected text features and boosting classifiers. In Information and Knowledge Technology (IKT), 2015 7th Conference on (pp. 1-5). IEEE.

[48] Kim, K., Sin-Eon, S., Jo, J., & Choi, S. H. (2015). SMS Spam filtering using Keyword Frequency Ratio. International Journal of Security and its Applications, 9(1), 329-36.

[49] Mahmoud, T. M., & Mahfouz, A. M. (2012). SMS spam filtering technique based on artificial immune system. IJCSI International Journal of Computer Science Issues, 9(1), 589-597.

[50] Mujtaba, G., & Yasin, M. (2014). SMS spam detection using simple message content features. J. Basic Appl. Sci. Res, 4(4), 275-279.

[51] http://www.grumbletext.co.uk, en son erişim tarihi : 13.02.2018