
GAZİ ÜNİVERSİTESİ
Gazi
1926

METİN VERİLERİNDE İÇERİK TABANLI SPAM TESPİTİ

Hamdullah KARAMOLLAOĞLU

YÜKSEK LİSANS TEZİ
BİLGİSAYAR BİLİMLERİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

Kasım 2019

Hamdullah K.ARAMOLLAOĞLU tarafından hazırlanan "METİN VERİLERİNDE İÇERİK TABANLI SPAM TESPİTİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilgisayar Bilimleri Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. İbrahim Alı:,er DOĞRU
Teknoloji Fakültesi, Gazi Üniversitesi
Bu tezin, kapsam ve kalite ı.,,,,,..k Y, •• Lisans Tezi olduğunu onaylıyorum.

Başkan: Prof. Dr. M. Ali AKÇAYOL
Mühendislik Fakültesi, Gazi Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum.

Üye: Dr. Öğretim Üyesi Mustafa SERT
Mühendislik Fakültesi, Başkent Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum.

Tez Savunma Tarihi: 28/11/2019

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları y rine getirdiğini onaylıyorum.

Doç. Dr. Aslıhan TÜFEKÇİ
Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

Bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Hamdullah KARAMOLLAOĞLU

28/11/2019

METİN VERİLERİNDE İÇERİK TABANLI SPAM TESPİTİ

(Yüksek Lisans Tezi)

Hamdullah KARAMOLLAOĞLU

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Kasım 2019

ÖZET

Twitter, en popüler sosyal medya platformlarından birisidir. Twitter kullanımının yaygınlaşması bir takım problemleri de beraberinde getirmiştir. Çoğu kez rahatsız edici ve zaman kaybettirici olan ve iletişim ortamının kaynaklarını boşa harcayarak gereksiz yer kaplayan bu spam tweet'ler bu problemlerin başında gelmektedir. Çalışmada, sosyal medya platformlarından Twitter üzerinde spam mesajların tespit edilmesi amaçlanmıştır. Makine Öğrenmesi modellerinden Vektör Uzay Modeli ile Türkçe ve İngilizce yazılmış tweet'ler üzerinde ayrı ayrı spam tespiti gerçekleştirilmiştir. Bu amaçla İngilizce tweet'ler üzerinde spam analizi için çeşitli platformlardan elde edilip oluşturulan eğitim ve sorgu amaçlı veri seti ve Türkçe tweet'ler üzerinde spam analizi için çeşitli platformlardan elde edilen veri setlerinin birleştirilmesi ile oluşturulan bir veri seti oluşturulmuştur. Verisetleri üzerinde yapılan spam tespiti sonucunda İngilizce tweet'ler üzerinde Vektör Uzay Modeli ile yapılan spam tespit çalışmasında %92, aynı yöntem ile Türkçe tweet'ler üzerinde yapılan spam tespiti çalışmasında %97'lik başarım oranı ile spam tespiti gerçekleştirilmiştir. Vektör Uzay Modelinin yanısıra WEKA kullanılarak Naive Bayes, SMO, IB1, Random Forest, Logistic ve J48 yöntemleri de ilgili probleme uygulanmıştır. Bu yöntemlerin arasından en başarılı olanların Naive Bayes (%93) ve Random Forest (%94) yöntemleri olduğu görülmüştür.

Bilim Kodu	:	92429
Anahtar Kelimeler	:	Vektör uzay modeli, makine öğrenmesi, spam tespiti
Sayfa Adedi	:	59
Danışman	:	Doç. Dr. İbrahim Alper DOĞRU

CONTENT BASED SPAM DETECTION IN TEXT DATA

(M. Sc. Thesis)

Hamdullah KARAMOLLAOĞLU

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

November 2019

ABSTRACT

Twitter is one of the most popular social media platforms. The widespread use of Twitter has brought some problems. These unwanted (spam) tweets are often annoying and time-consuming and take up unnecessary space by wasting resources of the communication environment. In this study, it is aimed to detect spam messages on social media platforms Twitter. Separate spam detection was performed on the Vector Space Model, one of the Machine Learning Methods, on tweets written in Turkish and English. For this purpose, a dataset was created by combining datasets obtained from various platforms for spam analysis on English tweets and for training and query purposes on Turkish tweets. As a result of spam detection on datasets, 92% spam detection was performed on English tweets with the Vector Space Model and 97% spam detection on Turkish tweets using the same method. In addition to Vector Space Model, Naive Bayes, SMO, IB1, Random Forest, Logistic and J48 methods were applied to the related problem by using WEKA. Naive Bayes (93%) and Random Forest (94%) were the most successful methods.

Science Code	:	92429
Key Words	:	Vector space model, machine learning, spam detection
Page Number	:	59
Supervisor	:	Assoc. Prof. Dr. İbrahim Alper DOĞRU

TEŞEKKÜR

Çalışmanın yürütülmesinde tez danışmanlığımı üstlenerek kıymetli zamanını ayırıp sabırla ve ilgiyle bana yol gösteren, değerli hocam; Doç. Dr. İbrahim Alper Doğru'ya teşekkür ederim. Ayrıca manevi desteklerini her zaman yanımda hissettiğim anneme ve babama; araştırma sürecim boyunca her türlü yardımını aldığım sevgili eşime en içten dileklerimle şükranlarımı sunuyorum.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

İÇİNDEKİLER vii

ÇİZELGELERİN LİSTESİ ix

ŞEKİLLERİN LİSTESİ x

KISALTMALAR xii

1. GİRİŞ 1

2. LİTERATÜRDE YER ALAN ÇALIŞMALAR 3

3. SOSYAL MEDYA VE TWITTER 9

3.1. Sosyal Medya Kullanım Oranları 9

3.2. Twitter ve Twitter İstatistikleri 11

4. MATERYAL VE YÖNTEM 13

4.1. Çalışmada Kullanılan Verisetleri 13

4.2. Yönteme İlişkin Teorik Temeller 14

4.2.1. Makine öğrenmesi metotları 14

4.2.2. Sınıflandırma 17

4.3. Yöntemin Uygulanması 18

4.3.1. Yönteme ilişkin işlem adımları 20

4.3.2. Twitter uygulama programlama arayüzü (Twitter API) 21

4.3.3. Twitter verilerine erişme 21

4.3.4. Verilerin ön-işlem aşamasından geçirilmesi 25

4.3.5. Vektör uzay modeli 33

Sayfa

4.3.6. Tweet içeriğindeki kötücül linklerin tespit edilmesi 40

4.4. Deneysel Çalışmaya İlişkin Başarım Oranları..... 44

4.4.1. Türkçe içerikli tweet'ler için geliştirilen uygulama..... 44

4.4.2. İngilizce içerikli tweet'ler için geliştirilen uygulama..... 46

4.4.3. WEKA ve yapılan çalışmanın WEKA ile karşılaştırılması 48

5. SONUÇ 53

KAYNAKLAR 54

ÖZGEÇMİŞ 59

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 2.1. Literatürde yer alan bazı spam tespit çalışmaları 6

Çizelge 3.1. Dünya nüfusunun sosyal medya kullanıcı sayıları 10

Çizelge 3.2. Türkiye nüfusunun sosyal medya kullanıcı sayıları 10

Çizelge 3.3. Bazı web siteleri ve her ziyarette ortalama harcanan zaman 11

Çizelge 4.1. Literatürde spam ileti tespiti çalışmalarında kullanılan örnek verisetleri... 13

Çizelge 4.2. Twitter API ile erişilebilen bazı nitelikler..... 21

Çizelge 4.3. API keyler sayesinde erişilen örnek twitter verileri 24

Çizelge 4.4. D_1, D_2 ve Q örnek belge içerikleri 36

Çizelge 4.5. Ön işlemden geçirilmiş ve kelimelerine ayrılmış D_1, D_2 ve Q belgeleri ... 37

Çizelge 4.6. Terim frekanslarının hesaplanması..... 37

Çizelge 4.7. Terim ağırlıklarının hesaplanması 38

Çizelge 4.8. Kötücül içeriklerin yer aldığı bazı web adresleri..... 40

Çizelge 4.9. Bazı link kısaltma siteleri ve oluşturdukları örnek kısa linkler 41

Çizelge 4.10. Bazı güvenlik araçları ve web adresleri..... 42

Çizelge 4.11. Türkçe verisetine ilişkin içerik bilgileri 44

Çizelge 4.12 Karmaşıklık matrisi 45

Çizelge 4.13. Performans başarım oranları..... 45

Çizelge 4.14. Performans hata oranları 46

Çizelge 4.15. İngilizce verisetine ilişkin içerik bilgileri 46

Çizelge 4.16. Karmaşıklık matrisi 46

Çizelge 4.17. Performans başarım oranları..... 47

Çizelge 4.18. Performans hata oranları..... 47

Çizelge 4.19. WEKA kullanılarak gerçekleştirilen çalışmaya ait başarım oranları 51

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 3.1. 2019 yılı için ülkemizde en çok kullanılan sosyal medya platformları 10

Şekil 4.1. Makine öğrenmesi yöntemlerinin sınıflandırılması 14

Şekil 4.2. Danışmanlı öğrenme 15

Şekil 4.3. Danışmansız öğrenme 16

Şekil 4.4. Yarı danışmanlı öğrenme 16

Şekil 4.5. Takviyeli öğrenme 17

Şekil 4.6. Çalışmada hazırlanan uygulamaya ait ekran görüntüsü 18

Şekil 4.7. Test verileri için gerçekleştirilen analiz sonuçlarına ait örnek bir kesit 19

Şekil 4.8. Spam analizine ilişkin gerçekleştirilen işlem adımları 20

Şekil 4.9. Uygulama oluşturma ekranı 22

Şekil 4.10. Twitter API keylerine ait ekran görüntüsü 23

Şekil 4.11. Twitter'dan veri çekilmesi için kullanılan access ve consumer key'ler. 23

Şekil 4.12. Anlık tweet'lere erişimi sağlayan kod bloğu. 24

Şekil 4.13. Bir etiket hakkındaki tweet'leri elde etmek için kullanılabilen kod bloğu... 24

Şekil 4.14. Harf olmayan gereksiz karakterlerin yerine boşluk eklenmesi..... 26

Şekil 4.15. Türkçede yer alan durma sözcükleri (stop words)..... 27

Şekil 4.16. İngilizcede yer alan durma sözcükleri (stop words). 27

Şekil 4.17. İngilizce sözcüklerin köklerine indirgenmesi için kullanılan kod bloğu..... 28

Şekil 4.18. Kökleri elde edilmiş örnek İngilizce kellimeler 28

Şekil 4.19. Türkçe kelimelerin kök hallerinin elde edilmesi 29

Şekil 4.20. Uygulamada yer alan Türkçe içerikli spam verisetine ait bir kesit 30

Şekil 4.21. Türkçe spam verisetinde yer alan kelimelerin kök halleri..... 31

Şekil 4.22. Uygulamada yer alan Türkçe içerikli spam olmayan verisetine ait bir kesit 32

Şekil **Sayfa**

Şekil 4.23. Türkçe spam olmayan verisetinde yer alan kelimelerin kök halleri. 33

Şekil 4.24. D_1, D_2 ve Q örnek belgelerinin vektör uzayındaki konumları 35

Şekil 4.25. Kısa linklerin normal (uzun) hale çevriren kod bloğu 42

Şekil 4.26. Googlesafebrowsing API'sinin kullanılması için oluşturulan kod bloğu 43

Şekil 4.27. Bir web sitesinin kötücül olup olmadığını belirleyen kod bloğu 43

Şekil 4.28 Girilen bir web sitesinin içeriğinde yer alan linkleri tespit eden kod bloğu .. 44

Şekil 4.29. Test verileri için gerçekleştirilen analiz sonuçlarına ait örnek bir kesit 48

Şekil 4.30. WEKA'ya ait giriş ekran görüntüsü 49

Şekil 4.31. Örnek bir arff dosyası 50

Şekil 4.32. WEKA'nın içeriğindeki bazı algoritmalar 50

Şekil 4.33. Weka 3.7.0 kullanılarak geliştirilen uygulamaya ilişkin örnek bir kesit 51

KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
API	Uygulama programlama arayüzü (App. programming interface)
ARFF	Öznitelik dosya biçimi (Attribute file format)
ID	Kimlik numarası **(**Identification number)
IDF	Ters terim frekansı **(**Inverse term frequency)
JSON	JavaScript nesnesi gösterimi (Javascript object notation)
K-NN	K-en yakın komşu (K-nearest neighbors)
SMS	Kısa mesaj (Short message)
SVM	Destek vektör makinası (Support vektor machine)
TF	Terim frekansı (Term frequency)
URL	Tekdüzen kaynak bulucu (Uniform resource locator)

1. GİRİŞ

İnternet kullanımının artması ve Web 2.0 teknolojisi ile birlikte insanların bilgisayar kullanım biçimlerinde değişiklik yaratmıştır. İnternet araştırma, inceleme ve eğlenme amaçlı kullanmakla birlikte artık kullanıcıların fikirlerini paylaşabildiği ve bu paylaşımlara geri dönüş alabileceği bir etkileşim ortamı sağlamaktadır.

Web 2.0 teknolojisi, sosyal medya denilen paylaşım ağlarının oluşmasına ve hızla yaygınlaşmasına ortam sağlamıştır. Sosyal medya ile beraber kullanıcılar bir konudaki görüş, öneri ve duygularını hızla başkalarıyla paylaşma imkanı bulmuş ve insanların birbirleriyle hızlı bir şekilde etkileşim kurmaları sağlanmıştır.

Sosyal medya ağları kullanım amaçları ve hedef kitle bakımından çeşitlilik sergilemektedir. Bazı sosyal ağlar fotoğraf paylaşımı üzerine kurulmuşken, bazıları video ve bilgi paylaşımı üzerine kurulmuştur. En yaygın sosyal medya platformları, Facebook, Youtube, Twitter, Instagram, Tumblr, Google+, Linkedln vb. paylaşım ağlarıdır.

Ülkemizde 2019 yılında, nüfusun %72'si internet kullanmakta, nüfusun %63'ü aktif olarak sosyal medya kullanmakta ve nüfusun %53'ünü aktif olarak mobil sosyal medya kullanmaktadır [1]. Sosyal medyanın çağımızın son derece yaygın iletişim araçlarından birisi olması bazı pazarlamacıların sosyal medyayı ticari bir araç olarak görmelerine; ürünleri ve hizmetleri ile ilgili çeşitli vaatler içeren reklam mesajlarını sosyal medya yoluyla kitlelere ulaştırmak istemelerine neden olmuştur.

Ürün reklamı yapmak sokaklarda bildiri dağıtmaya benzetilse de reklamı yapılan ürünün kalitesi, kanun ve standartlara uygunluk durumu, tüketici hakları güvence altına alıp almadığı gibi hususlarda ilgili reklam ile ürün arasında hukuksal bir ilişki kurulamadığından sosyal medya üzerinden yapılan reklamlarda sahtecilik ve dolandırıcılık riski çok fazladır.

Sosyal medya iletilerinde yer alan diğer bir tehlike de kötücül yazılımlar vasıtasıyla bilgisayarın uzaktaki bir kişinin kontrolüne geçmesine neden olan, bot (kurtçuk, yazılım robotu) adı verilen kötücül yazılımların sosyal medyada paylaşılan ve bir sayfaya yönlendirme yapan linkler vasıtasıyla kolayca yayılabilmesidir. Bu kötücül yazılımlar bulaştığı bilgisayarları kontrol altına alarak kullanıcıların haberi olmadan bilgi çalmak vb. işlerde kullanılmaktadır [2].

Kişilerin izni ve isteği dışında gönderilen sosyal medya iletileri, bir konuda kamuoyu oluşturmak amaçlı olabileceği gibi bahis ve pornografik içerikli sitelere yönlendirme yapmak için web ilanı şeklinde de oluşturulmuş olabilmektedir. Çoğu kez rahatsız edici ve zaman kaybettirici olan ve iletişim ortamının kaynaklarını boşa harcayarak gereksiz yer kaplayan bu istenmeyen sosyal medya iletileri 'spam' olarak adlandırılırlar.

Çalışmada Türkçe ve İngilizce yazılmış Twitter iletileri üzerinde spam tespiti işleminin gerçekleştirilmesi amaçlanmıştır. Twitter spam içeriklerin en çok yer aldığı sosyal medya platformlarından birisidir. Twitter'ın araştırmacılara sağladığı Twitter API sayesinde, Twitter iletileri (tweet'ler) istenilen bir ortama kaydedilebilmekte ve çeşitli yöntemler ile analiz edilebilmektedir.

Literatürdeki çalışmalar incelendiğinde genelde İngilizce içerikli iletiler üzerinde, makine öğrenmesi yöntemleri kullanılarak spam ileti tespiti yapılmaktadır. Türkçe içerikler üzerinde yapılan akademik çalışmaların sayısı çok azdır. Bu çalışmada İngilizce içerikli iletilerin yanı sıra Türkçe içerikli iletiler için de spam tespitinin gerçekleştirilmesi amaçlanmıştır.

İkinci bölümde, literatürde yapılan çalışmalar ele alınmıştır. Üçüncü bölümde sosyal medya platformlarından, çeşitli Twitter istatistikleri, Twitter mimarisi ve Twitter'dan verilerin çekilmesi için gerekli aşamalardan bahsedilmiştir. Dördüncü bölümde ise ayrıntılı bir şekilde çalışmada yer alan yöntem ve araçlar ile bu araçlar kullanılarak yapılan deneysel çalışma ve sonuçları belirtilmiştir. Son bölümde ise önerilen modelin başarısı ve elde edilen sonuçlar değerlendirilmiştir.

2. LİTERATÜRDE YER ALAN ÇALIŞMALAR

Literatürdeki spam tespiti çalışmalarına bakıldığında, çalışmaların genellikle İngilizce iletiler ile oluşturulmuş verisetleri üzerinde makine öğrenmesi yöntemleri uygulanarak yapıldığı görülmektedir.

Liew vd. [3] 2019 yılında Random Forest yöntemi ve 200 kötücül URL linki kullanarak yaptıkları spam tweet tespiti çalışmasında %94,75 oranında başarım ile sınıflandırma işlemi gerçekleştirilmiştir.

Gunawan vd. [4] 2019 yılında 860 tanesi spam, 125 tanesi spam olmayan olmak üzere toplam 985 metin mesajı kullanılarak Twitter-LDA algoritması yardımıyla yaptıkları spam tespit çalışmasında %96,49 oranında bir başarım ile doğru sınıflandırma işlemi gerçekleştirilmiştir.

Nauta [5] 2016 yılında hesapları ele geçirilmiş Twitter kullanıcıların tespiti için yaptığı çalışmada 2715 tanesi normal ve 983 tanesi ele geçirilmiş hesaplardan oluşan bir veri seti kullanılmıştır. SMO ve J48 metotlarını kullanarak yaptığı ele geçirilmiş Twitter kullanıcı hesaplarının tespiti çalışmasında, makine öğrenmesi yöntemlerinden SMO'yu kullanarak %96,106 ve J48'i kullanarak %99,351 oranında bir başarım ile doğru sınıflandırma işlemi gerçekleştirilmiştir.

Perveen vd. [6] 2016 yılında 30 bin tweet üzerinde duygu ve içerik bazlı özellikler ve beş ayrı makine öğrenmesi yöntemi (BayesNet, Naive Bayes, Random Forest, J48 ve SVM) yardımıyla yaptıkları Twitter üzerinde spam tespiti çalışmasında yaklaşık %90-91 oranında bir başarı ile doğru sınıflandırma işlemi gerçekleştirilmiştir.

Cao ve Caverlee [7] 2015 yılında tweetlerde yer alan URL'leri gönderen kullanıcıların ve bu gönderilere tıklayan kullanıcılar üzerinde yaptıkları davranış bazlı analiz ile spam tweet'lerin tespiti gerçekleştirilmiştir. Sonuçta %86 oranında bir başarı ile doğru sınıflandırma işlemi gerçekleştirilmiştir.

Wang vd. [8] 2015 yılında yaptıkları çalışmada, iki adet veri seti kullanmışlardır. İlk veri seti 20707 adet spam ve 19249 normal tweet ve ikinci veri seti 1000 adet spam ve 9828 adet normal tweet içermektedir. Yapılan çalışmada Naive Bayes, K-En Yakın Komşuluk, Karar Destek Makineleri, Karar Ağaçları ve Rastgele Orman Metodları kullanılmıştır. En iyi sınıflandırma %94,6 başarım oranı ile Rastgele Orman metodu ile elde edilmiştir.

Hu vd. [9] 2014 yılında yaptıkları çalışmada TAMU Social Honeypots Dataset ve Twitter Suspended Spammers Dataset adlı verisetlerini kullnarak yaptıkları çalışmada twitter mesajları üzerinde spam mesaj atan kullanıcıların tespitinin yapılmasını amaçlamışlardır. LS Content (the Least Squares) metodunu kullanarak yaptıkları çalışmada %85 civarında bir doğruluk ile spam kullanıcı tespiti işlemini gerçekleştirmişlerdir.

Martinez-Romo vd. [10] 2013 yılında yaptıkları çalışmada, toplamda 20 milyon tweet üzerinde yaptıkları çalışmada, Karar Ağaçları, Naive Bayes, Lojistik Regresyon, Rastgele Orman metodlarını kullanarak gerçekleştirdikleri içerik bazlı kötücül tweet tespiti analizi ile %94,5'lik bir başarım oranı ile sınıflandırma işlemi gerçekleştirilmiştir.

Sangho ve Jong [11] 2012 yılında Twitter üzerinden topladıkları veriler ile oluşturdukları 224,834 adet tweet içeren eğitim ve 174,259 adet tweet içeren test veri seti kullanılmıştır. Bu verisetleri üzerinde LIBLINEAR Kütüphanesi ve Logistic Regression (LR) metodu kullanılarak yaptıkları tweet içeriğindeki kötücül linklerin tespiti çalışmasında % 91,10'luk bir başarım elde doğru sınıflandırma gerçekleştirilmiştir.

Jong vd. [12] 2011 yılında twitter üzerinden çeşitli zaman dilimlerinde elde ettikleri 267,551 tweet üzerinde Bagging, LibSVM, J48, BayesNet ve FT yöntemleri ile yaptıkları spam tweet tespiti çalışmasında %93-%95 oranında bir başarım elde edilmiştir.

McCord vd. [13] 2011 yılında 1000 adet twitter kullanıcısı üzerinde yaptıkları spam kullanıcıların tespiti çalışmasında Rastgele Orman, Destek Vektör Makineleri, K-En yakın Komşu ve Naive Bayes metodları kullanılmıştır. Rastgele Orman metodu %95'lik başarı oranı ile en iyi sınıflama yapan yöntem olduğu görülmüştür.

Benevenuto vd. [14] 2010 yılında yaptıkları çalışmada, #musicmonday, #MichaelJackson, ve #SusanBoyle gibi popüler hastagler içeren yaklaşık 1.7 milyar tweet veri seti olarak elde edilmiştir. Destek Vektör Makineleri metodu ile spam kullanıcıların %70'i doğru tespit edilmiştir.

Kyumin vd. [15] 2010 yılında yaptıkları çalışmada, Twitterda spam içerik oluşturan kullanıcıların profillerinin belirlenmesi ve bu profillere göre filtreleme yapılması amacıyla balküpü (honeypot) oluşturmuşlardır. Bu amaçla belirledikleri 500 kullanıcı için Ağustos-Eylül 2009 tarihleri arasında ilgili kullanıcıların attıkları tweetler incelenmiştir. Yaptıkları çalışma sonucunda %88,98 oranında bir başarım ile Twitter üzerinde spam içerik oluşturan kullanıcıların tespiti gerçekleştirilmiştir.

Sethi ve Bhootna [16] tarafından yapılan çalışmada, spam mesaj tespiti için Bayes Sınıflandırıcı yönteminden yararlanılmıştır. 100 adet mesaj eğitim amaçlı, 100'den fazla mesaj ise sınıflandırma ve test işlemleri için kullanılarak %97,4'lik bir başarı oranı ile spam tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir.

Ezpeleta vd. [17] tarafından yapılan spam mesaj tespiti çalışmasında, sözlük tabanlı duygu analizi ve TextBlob Sınıflandırıcıdan yararlanılmıştır. Veri seti olarak 492 pozitif ve 394 negatif veri içeren 'SemEval-2013' ile 747 spam ve 4827 normal mesaj içeren 'SMS Spam Collection' veri seti kullanılmıştır. Sonuçta %98,76'lık bir başarı oranı ile spam tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir.

Yang vd. [18] tarafından Bayes Sınıflandırıcı kullanılarak yapılan çalışmada eğitim ve test işlemleri için 2000 spam ve 2000 spam olmayan mesaj kullanılmıştır. Sonuçta %97,90'lık bir başarı oranı ile spam tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir.

Bozan vd. [19] tarafından yapılan çalışmada 'SMS Spam Collection' veri seti kullanılarak Naïve Bayes Sınıflandırıcı, Karar Destek Makinesi (SVM) ve K-En Yakın Komşu (k-NN) metotları yardımıyla spam tespiti amaçlanmıştır. Sonuçta Naïve Bayes Sınıflandırıcı kullanılarak %97.55, SVM kullanılarak %98,61 ve k-NN kullanılarak %93,35'lik bir başarı oranı ile spam tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir.

Akbari ve Sajedi [20] tarafından 747 adet spam ve 4825 adet spam olmayan mesaj içeren veri seti kullanılarak GentleBoost metodu yardımıyla yapılan spam tespiti çalışmasında %98,30'luk bir başarı oranı ile spam tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir.

Li ve Zeng [21] tarafından 12000 spam ve 8000 spam olmayan mesaj içeren veri seti kullanılarak Vektör Uzay Modeli yardımıyla yapılan çalışmada yaklaşık %89'luk bir başarı oranı ile spam tespiti ve sınıflandırılması işlemi gerçekleştirilmiştir.

Wang [22] tarafından 2010 yılında yapılan Twitter üzerinde gerçekleştirilen spam tespiti çalışmasında 500000 tweet veri seti olarak oluşturulmuştur. İlgili veri seti üzerinde Naive Bayes, Yapay Sinir Ağları, Karar Destek Makineleri ve Karar ağaçları kullanılarak spam tespit işlemi gerçekleştirilmiş ve sonuç olarak %89 oranında bir başarım ile sınıflandırma işlemi gerçekleştirilmiştir.

Literatürde Türkçe içererikli verisetleri kullaılarak yapılan çalışmaların kısıtlı olduğu görülmektedir. Türkçe içerikli yapılan çalışmalar genellikle e-posta ve SMS içerikleri için makine öğrenmesi yöntemleri ile gerçekleştirilen spam tespiti çalışmalarıdır.

Karasoy ve Ballı [23] tarafından 2016 yılında Türkçe içerikli SMS'ler üzerinde Random Forest algoritması kullanılarak yapılan spam tespiti çalışmasında %93,76 oaranında bir başarım ile sınıflandırma işlemi gerçekleştirilmiştir.

Özdemir vd. [24] tarafından 2013 yılında Türkçe mail içerikleri üzerinde CSCA algoritması kullanılarak yapılan spam tespiti çalışmasında %86 oranında bir başarım ile sınıflandırma işlemi gerçekleştirilmiştir.

Çalış vd. [25] tarafından 2013 yılında Türkçe içerikli e-postalar üzerinde k-NN algoritması kullanılarak yapılan spam tespiti çalışmasında %96,5 oaranında bir başarım ile sınıflandırma işlemi gerçekleştirilmiştir.

Literatürde spam tespiti çalışmaları incelendiğinde kullanılan verisetlerinin kısıtlı olduğu görülmektedir. Spam tespiti alanındaki çalışmaların genelikle İngilizce içerikli iletiler için yapıldığı, Türkçe içerikli verisetlerinin sayısının az olduğu görülmektedir. Literatürde Türkçe verisetlerinin az olması Türkçe için yapılan spam tespiti çalışmalarının da az olmasına sebebiyet vermektedir.

Çizelge 2.1'de literatürde yer alan spam tespit çalışmalarından bazılarına ilişkin kullanılan yöntemler, verisetleri ve çalışmaların başarım oranları görülmektedir.

Çizelge 2.1. Literatürde yer alan bazı spam tespit çalışmaları

Çalışma	**Yöntemler**	**Veriseti**	**Başarım Oranı**
Benevenuto vd. [14]	Destek Vektör Makineleri	1.7 milyar tweet içeren veriseti	%70
McCord vd. [13]	Rastgele Orman, Destek Vektör Makineleri, K-En yakın Komşu, Naive Bayes	1000 adet twitter kullanıcısının attığı tweetler	%95
Hu vd. [9]	LS Content (the Least Squares) metodu	TAMU Social Honeypots Dataset ve Twitter Suspended Spammers Dataset adlı verisetleri	%85

Çizelge 2.1. (devam) Literatürde yer alan bazı spam tespit çalışmaları

Çalışma	Yöntemler	Veriseti	Başarım Oranı
Kyumin vd. [15]	Balküpü (honeypot)	500 adet twitter kullanıcısının attığı tweetler	%88,9
Sangho ve Jong [11]	LIBLINEAR kütüphanesi ve Logistic Regression (LR) metodu	224,834 adet tweet içeren eğitim ve 174,259 adet tweet içeren test veri seti	%91,1
Song vd. [12]	Bagging, LibSVM, J48, BayesNet ve FT yöntemleri	267,551 tweet içeren veriseti	%95
Gunawan vd. [4]	Twitter-LDA algoritması	860 tanesi spam, 125 tanesi spam olmayan olmak üzere toplam 985 metin mesajı	%96,4
Liew vd. [3]	Random Forest yöntemi	200 kötücül URL linki	%94,7
Perveen vd. [6]	BayesNet, Naive Bayes, Random Forest, J48 ve SVM	30 bin tweet içeren veriseti	%91
Nauta [5]	SMO ve J48	2715 tanesi normal ve 983 tanesi ele geçirilmiş hesaplardan oluşan bir veri seti	%99
Wang vd. [22]	Naive Bayes, K-En Yakın Komşuluk, Karar Destek Makineleri, Karar Ağaçları ve Rastgele Orman Metodları	20707 adet spam ve 19249 normal tweet ve 1000 adet spam ve 9828 adet normal tweet içeren verisetleri	%94,6
Sethi ve Bhootna [16]	Bayes Sınıflandırıcı	200 adet spam/spam olmayan mesaj içeren veriseti	%97,4
Bozan vd. [19]	Naive Bayes, SVM, K-NN	SMS Spam Collection dataset	%98,6
Özdemir vd. [24]	CSCA algoritması	929 adet e-posta içeriği	%86
Çalış vd. [25]	K-NN algoritması	400 normal 400 spam toplam 800 adet eposta içeriği	%96,5
Karasoy ve Ballı [23]	Random Forest algoritması	5333 adet SMS içeriği	%93,7

Çizelge 2.1'de görüldüğü gibi literatürdeki çalışmalarda genellikle makine öğrenmesi yöntemleri çeşitli verisetleri üzerine uygulanarak spam mesajların tespit edilme işlemi gerçekleştirilmiştir.

3. SOSYAL MEDYA VE TWITTER

Sosyal medya platformlarında geleneksel medya araçlarında yer alan yayın standart süresi benzeri bir engel olmamasından dolayı bilgiye erişim hızı yönünden sosyal medyayı ön plana çıkarmaktadır.

Sosyal medyanın iletişim kurma fonksiyonu sayesinde kullanıcıların birbirleri arasında haberleşmeleri sağlanmaktadır. Bu haberleşme, dahil olunan sanal topluluğa kitlesel mesaj verme fırsatı da tanımaktadır.

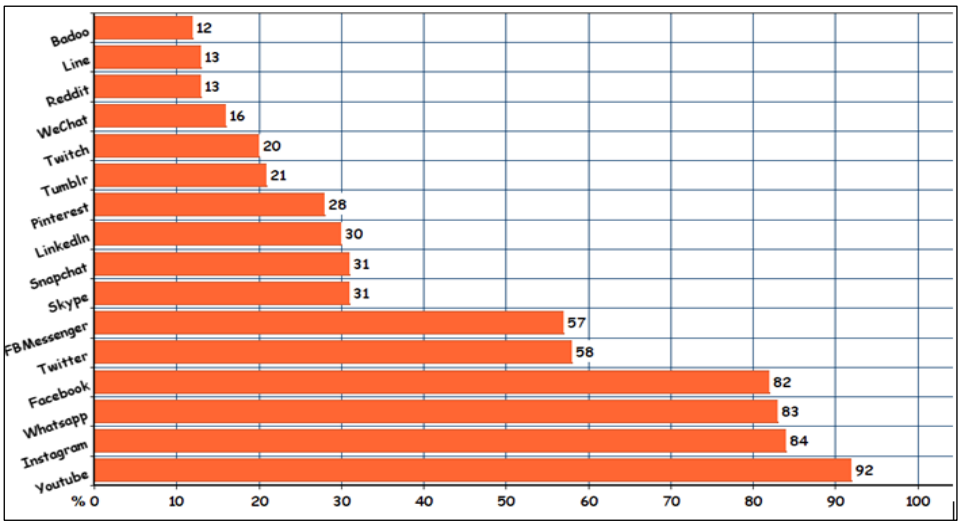
Sosyal medya platformları sağladıkları yazılı, sesli mesajların yanısıra video ve fotoğraf paylaşımı seçenekleri de sunması sanal bir eğlence ortamı sağlamakta aynı zamanda diğer kullanıcılarla etkileşim içerisine girip arkadaşlık kurabilmektedir.

Sosyal medya platformları ayrıca kullanıcılara özgürce gündem belirleme ve bir konu hakkında kamuoyu oluşturma imkanı sağlamaktadır. İçerdiği geniş bilgi yelpazesi ile de araştırmacılar için çeşitli araştırma ve incelemeler yapma imkanı sağlamaktadır [26].

Tüm bunların yanında çeşitli firmaların reklam amaçlı içerik oluşturarak kitlelere ulaşma amacıyla da kullanılan sosyal medya; kumar, bahis ve pornografik içerik oluşturan bazı kötü niyetli kullanıcıların da çoğunlukla içerik paylaştıkları ortam haline gelmiştir. Çeşitli etiketler altında spam mesajlar oluşturarak belirli web sayfalarına yönlendirme yapan linklerin yanısıra fotoğraflar ve videolar ile de çeşitli ürün reklamı yapmak üzere oluşturulmuş hesaplar ve içerikler de mevcuttur.

3.1. Sosyal Medya Kullanım Oranları

İnternet ve mobil cihaz kullanıcı sayısındaki artış sosyal medya ağlarının kullanımını da gün geçtikçe artırmaktadır. Şekil 3.1'de 2019 yılında ülkemizde en çok kullanılan sosyal medya platformları görülmektedir.



Şekil 3.1. 2019 yılı için ülkemizde en çok kullanılan sosyal medya platformları [27]

Şekil 3.1'de görüldüğü gibi ülkemizde 2019 yılında en çok kullanılan sosyal medya platformları Youtube, Instagram, Whatsapp, Facebook ve Twitter'dır.

Dünyada ve ülkemizdeki toplam nüfus içerisinde mobil cihaz, internet ve sosyal medya kullanımı gün geçtikçe artarak yoluna devam etmektedir. Çizelge 3.1'de Dünya nüfusunun mobil cihaz, internet, sosyal medya kullanıcı sayıları görülmektedir.

Çizelge 3.1. Dünya nüfusunun sosyal medya kullanıcı sayıları [28]

Toplam Nüfus (2019 Yılı)	Mobil Cihaz Kullanıcı Sayısı	İnternet Kullanıcı Sayısı	Sosyal Medya Kullanıcı Sayısı	Mobil Sosyal Medya Kullanıcı Sayısı
7.676 Milyar	5.112 Milyar	4.388 Milyar	3.484 Milyar	3.256 Milyar

Çizelge 3.1'de görüldüğü gibi internet ve mobil cihaz kullanıcı sayısının fazla olması sosyal medya kullanım oranlarını da artırmaktadır. Ülkemizde Ocak 2019 yılında toplam nüfus içerisindeki mobil cihaz, internet ve sosyal medya kullanım oranları Çizelge 3.2'de görülmektedir.

Çizelge 3.2. Türkiye nüfusunun sosyal medya kullanıcı sayıları [28]

Toplam Nüfus (Ocak 2019 Yılı)	Mobil Cihaz Kullanıcı Sayısı	İnternet Kullanıcı Sayısı	Sosyal Medya Kullanıcı Sayısı	Mobil Sosyal Medya Kullanıcı Sayısı
82.44 Milyon	76.34 Milyon	59.36 Milyon	52.00 Milyon	44.00 Milyon

Çizelge 3.2'de görüldüğü gibi ülkemizde de sosyal medya kullanımı dünya genelinde olduğu gibi ülke nüfusuna oranla çok yüksek bir değerdedir.

Çizelge 3.3'de Bazı web siteleri için 2019 yılında Dünya genelinde kullanıcıların ilgili web siteleri ziyaret ettiğinde harcadıkları zaman görülmektedir.

Çizelge 3.3. 2019 yılında Bazı web siteleri ve her ziyarette ortalama harcanan zaman [28]

Web Sitesi	**Kategori**	**Her Ziyarette Ortalama Harcanan Zaman**
Google.com	Arama	9 dk 12 sn
Youtube.com	Video	21 dk 36 sn
Facebook.com	Sosyal	11 dk 44 s
Baidu.com	Arama	6 dk 53 s
Wikipedia.org	Referans	3 dk 45 sn
Yahoo.com	Portal	6 dk 26 sn
Twitter.com	Sosyal	9 dk 14 sn
Pornhub	Yetişkin	10 dk 16 sn
Yandex.ru	Arama	10 dk 43 sn
Instagram.com	Sosyal	6 dk 25 sn

Çizelge 3.3'te görüldüğü gibi sosyal medya platformlarında kullanıcılar uzun vakitler harcayabilmektedir.

Twitter sosyal medya platformları arasında en popüler olanlarından birisidir. Özellikle genç kullanıcılar, siyasiler ve diğer ünlüler tarafından kullanım oranları diğer sosyal medya platformlarına göre gün geçtikçe artmaktadır. Twitter'ın araştırmacılara sağladığı Twitter API'si sayesinde belirli sayıdaki Twitter iletileri istenilen bir ortama kaydedilebilmektedir.

3.2. Twitter ve Twitter İstatistikleri

Twitter, kullanıcıların en fazla 140 karakterden oluşmak kaydı ile duygu ve düşüncelerini, resim, video veya herhangi bir web linkini paylaşabildikleri bir sosyal medya platformudur. Bu platformda kullanıcılar birbirlerini takip edebilir veya başka kullanıcıların paylaşımlarını kendilerini takip eden kullanıcıların görebilmeleri için yeniden paylaşabilirler [29].

Twitter ve diğer sosyal medya platformlarının genel işlevleri; anlık bilgiye ulaşma, kişisel haberleşme, kitlesel mesaj verme, eğlence, arkadaş edinme, araştırma yapma, kamuoyu oluşturma ve gündem belirlemedir [26].

Twitter'da paylaşımların arkadaş listesi dışında, daha geniş kitlelere ulaşması için paylaşılan iletinin başına hastag olarak isimlendirilen "#" (diyez) karakteri getirilir. Aynı hastag içeren paylaşımlar çoğaldıkça sanal bir gündem oluşmakta ve o andaki popüler gündemin ne olduğu kullanıcılar tarafından görülebilmektedir [30].

Twitter’da yaygın olarak kullanılan karakterlerden birisi de “@” karakteridir. Bu karakterden sonra kullanıcı adı yazılarak, kullanıcıya direkt olarak yanıt verilebilmekte veya bir paylaşımda ilgili kullanıcı etiketlenebilmektedir [31].

Twitter’a ait güncel bazı güncel bilgiler şöyledir:

- 2019 yılı itibariyle Twitter’da günlük ortalama atılan tweet sayısı 500 milyon civarıdır.
- Similar Web’in araştırmasına göre Twitter dünyada en çok ziyaret edilen 7. sitedir.
- Twitter’da saniyede ortalama 5.787 tweet paylaşılmaktadır.
- Twitter‘da aylık aktif kullanıcı sayısı ortalama 326 milyondur.
- Kullanıcıların günlük aktif Twitter kullanım oranı yüzde 46'dır.
- Twitter'ın dünya çapında 35 ofisi yer almaktadır.
- Dünya genelinde 187 hükumet başkanı Twitter kullanmaktadır.
- Reklamcıların yaklaşık yüzde 75’i Twitter kullanmaktadır.
- İşletmelerin yaklaşık yüzde 85’i Twitter üzerinden hizmet sunma yolunun faydalı olacağını düşünmektedir.
- Twitterda yer alan reklamların televizyon reklamlarına göre yaklaşık %11 daha etkili olduğu gözlemlenmiştir.
- Twitter kullanıcılarının %60’ı erkek ve %40’ı kadındır.
- Dünyaya ünlü markalar 2018 yılı boyunca yaklaşık olarak ortalama 122 adet tweet atmıştır.
- Tanıtımı yapılan ürünlerde GIF içeren tweetler etkileşimi %55 arttırdığı görülmüştür.
- Video içeren tweet'ler etkileşim oranını 10 kat arttırmaktadır.
- Türkiye’de günlük paylaşılan tweet sayısı yaklaşık 7 milyondur.
- Türkiye'de en çok tweet paylaşan sektörler; teknoloji, tekstil ve bankacılıktır.
- Sosyal medya kullanıcı sayısı 2019 yılında 3,5 milyar civarına ulaşmıştır.

Twitter kullanımının son derece yaygın olması ve kullanıcıların uzun vakitler bu platformda zaman harcamaları, bazı kişi ve kuruluşların bu mecraları reklam amaçlı kullanmak istemelerine neden olmaktadır. Aynı zamanda kötü niyetli kişilerin Twitter’da bahis veya pornografik içeriklere yöneltme amaçlı reklam ve ilgili web sayfalarına yöneltici linkler oluşturmak kaydıyla spam iletiler (tweet’ler) ile sistemi gereksiz yere işgal etmekte ve kullanıcıların zamanını boşa harcamalarına neden olmaktadır.

4. MATERYAL VE YÖNTEM

Çalışmada, Twitter içeriklerinde yer alan spam iletilerin belirlenmesi amaçlanmaktadır. Türkçe ve İngilizce tweet içeriklerindeki spam iletilerin tespiti için iki ayrı çalışma yapılmıştır. Spam analizi için Makine Öğrenmesi modellerinden Vektör Uzay Modeli kullanılmıştır. Çalışmanın başarım tespiti için literatür taraması yapılmış ve spam analizi için spam/spam olmayan şeklinde etiketlenmiş iletiler şeklinde oluşturulmuş Türkçe içerikli 1250 ileti ve İngilizce içerikli 13269 iletinin yer aldığı verisetleri ilgili taramalar sonucu elde edilmiştir. İlgili verisetleri İngilizce ve Türkçe içerikler ayrı ayrı olmak üzere text dosyalarına kaydedilmiştir. Bu verisetleri üzerinde Vektör Uzay Modeli spam tespiti amaçlı olarak kullanılmıştır. Çalışmaya ilişkin yazılım Java Programlama dili ile Eclipse platformu üzerinde geliştirilmiştir.

4.1. Çalışmada Kullanılan Verisetleri

Literatürde Spam iletilerin tespiti çalışmalarında kullanılmak üzere oluşturulmuş verisetleri Çizelge 4.1'de görülmektedir.

Çizelge 4.1. Literatürde spam ileti tespiti çalışmalarında kullanılan örnek verisetleri

Veriseti	Kaynak
Caroline Tag Veriseti	[32]
TurkishSMS veriseti	[33]
National University of Singapore (NUS) Corpus	[34]
DIT SMS Spam Dataset	[35]
Malay SMS corpus	[36]
SMS Spam Corpus Collection	[37]
UCI SMS Spam	[38]
Deceptive Opinion Spam Corpus v1.4	[39]

Çizelge 4.1'de yer alan literatürdeki verisetlerinin çoğu İngilizce iletiler üzerinde spam tespiti yapılması için oluşturulmuştur. Çalışmanın başarım oranının tespiti için ilgili verisetleri içerisinden İngilizce spam tespit çalışması için 'SMS Spam Corpus Collection'

ve ‘UCI SMS’ verisetlerin derlenen 13269 ileti ile Türkçe spam tespit çalışması için ‘TurkishSMS’ veriseti ile çeşitli platformlardan derlenen toplam 1250 ileti içeren bir veriseti oluşturulmuştur. İlgili verisetlerindeki iletiler spam olup olmadıklarına göre hazır bir şekilde etiketli olarak araştırmacılara sunulmuştur. Çalışmada elde edilen etiketlenmiş iletilerden oluşan sonuçlar ile bu hazır etiketli olan verisetlerindeki iletiler karşılaştırılmıştır. Çalışmanın başarım oranı bu karşılaştırma sonucunda elde edilmiştir.

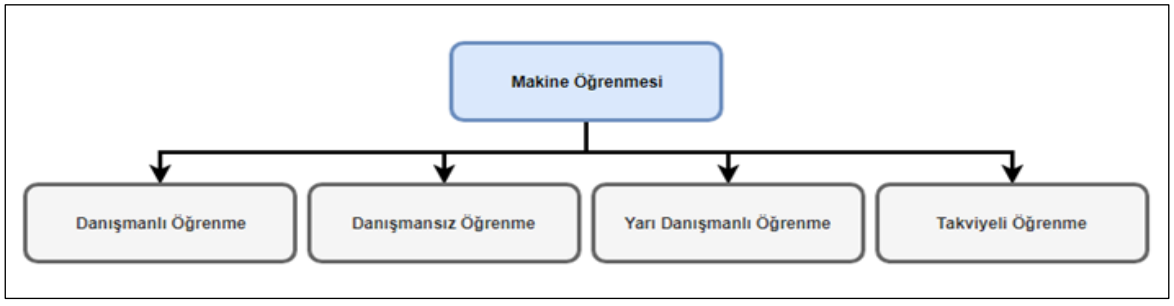
4.2. Yönteme İlişkin Teorik Temeller

Çalışmada Makine Öğrenmesi modellerinden Vektör Uzay Modeli kullanılmıştır. Makine Öğrenmesi geçmiş deneyimlerinden yola çıkarak bir model oluşturulmasına ve gelecekte karşılaşılan durumlardaki bilinmeyenlerin tahmin edilmesini sağlayan yapay zekâ alanıdır.

Makine öğrenmesinin birçok kullanım alanı vardır. Eğer makine öğrenmesi metotları büyük veritabanlarına uygulanırsa buna veri madenciliği ismi verilmektedir. Makine Öğrenmesi işlemlerinin gerçeklenmesi için temel adımlar, veri toplama, verilerin ön-işlenerek hazırlanması, modelin eğitilmesi, modelin değerlendirilmesi ve performans artırımı şeklindedir.

4.2.1. Makine öğrenmesi metotları

Makine Öğrenmesi Metotları eldeki verileri kullanarak en iyi modeli oluşturmaya ve yeni veriler geldikçe önceki veriler ile oluşturulan model yardımıyla yeni gelen verileri en doğru şekilde analiz etmeyi amaçlar. Makine Öğrenmesi Metotları yapısal özelliklerine göre çeşitlilik gösterirler. Şekil 4.1’de Makine Öğrenmesi Metotlarının sınıflandırılması görülmektedir [40].

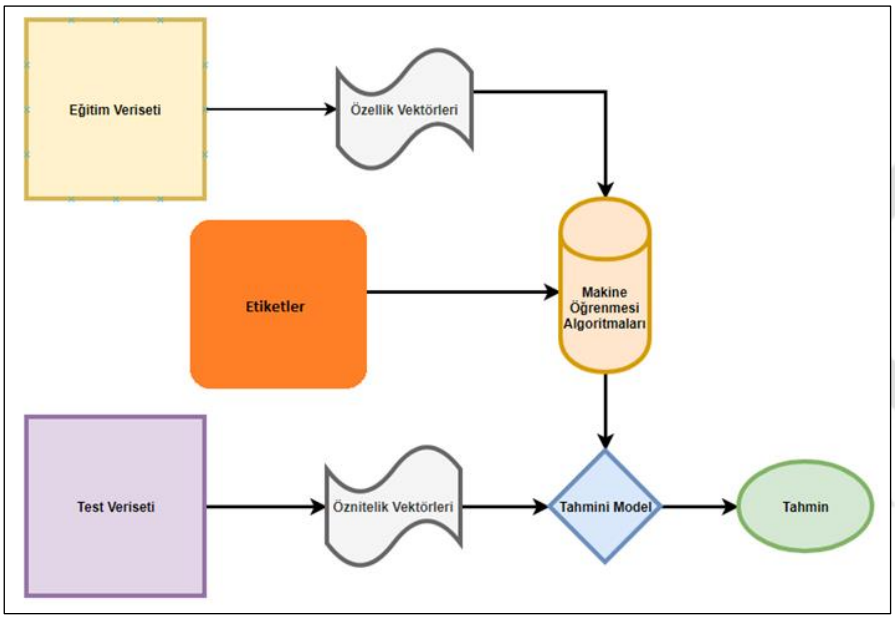


Şekil 4.1. Makine öğrenmesi yöntemlerinin sınıflandırılması

Şekil 4.1’de görüldüğü gibi Makine Öğrenmesi Yöntemleri; Danışmanlı, Danışmansız, Yarı Danışmanlı ve Takviyeli öğrenme olmak üzere dörde ayrılmaktadır.

Danışmanlı öğrenme

Danışmanlı öğrenme modelinde, eğitimle ilgili olaylar ve olaylara ilişkin örnekler girdi/çıktı olarak sisteme girilir. Eğitilmiş sistem tarafından oluşturulan model kullanılarak test veriseti üzerinde tahmin yapma amacıyla kullanılır. En çok bilinen danışmanlı öğrenme algoritmaları: Destek Vektör Makineleri, Yapay Sinir Ağları, Lojistik Regresyon, Naive Bayes, K-En Yakın Komşu, Rastgele Orman ve Karar Ağaçları'dır. Şekil 4.16'de Danışmanlı Öğrenmeye ait model görülmektedir [40].

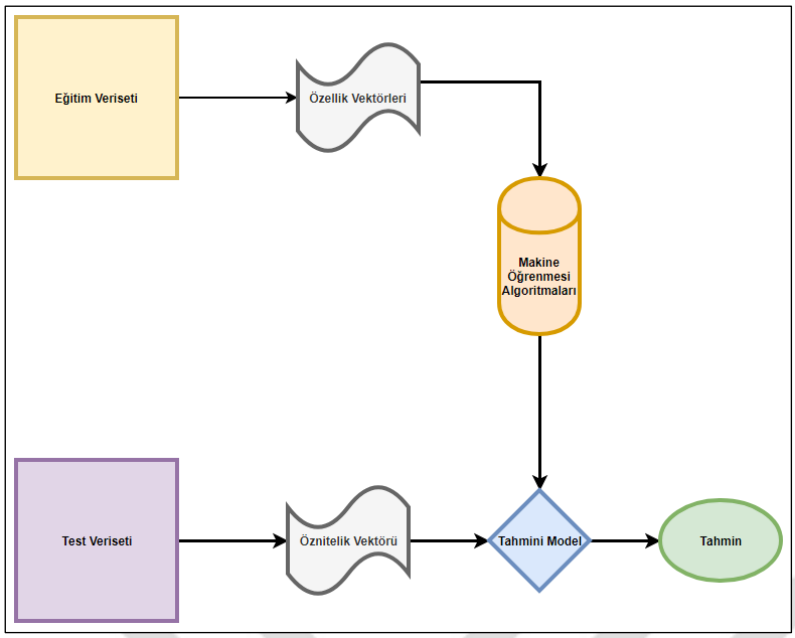


Şekil 4.2. Danışmanlı öğrenme

Şekil 4.2'de görüldüğü gibi Danışmanlı öğrenmede özellik vektörleri, etiketler ve tahmini modelden yararlanılarak bir tahmin gerçekleştirilir [40].

Danışmansız öğrenme

Danışmansız Öğrenme'de sisteme çıkışlardan bağımsız olarak sadece giriş bilgileri verilir. Sistem giriş bilgilerine ait örnekler arasındaki ilişkilerin bulunmasını sağlayarak bir model oluşturur. Burada amaç örnekler arasında ilişkiler kurularak kümeleme, olasılık yoğunluk tahmini, boyut indirgeme vs. gibi alanlardır. Şekil 4.17'te Danışmansız Öğrenme'ye ait model görülmektedir [40].

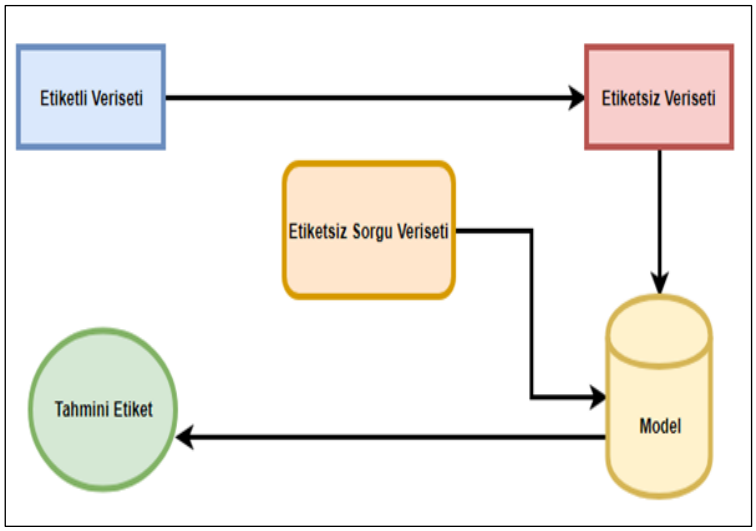


Şekil 4.3. Danışmansız öğrenme

Şekil 4.3'te görüldüğü gibi Danışmansız öğrenmede özellik vektörleri ve tahmini modelden yararlanılarak bir tahmin gerçekleştirilir.

Yarı danışmanlı öğrenme

Yarı Danışmanlı Öğrenme'de sisteme etiketlenmemiş verilerin yanında az miktarda etiketlenmiş veri girilmektedir. Bu öğrenme modeline ait metotlar genellikle, etiketlenmiş verinin az miktarda yer aldığı durumlarda etiketlenmemiş durumların tahminlenmesinde kullanılmaktadır [40]. Yarı Danışmanlı Öğrenme'ye ait model Şekil 4.4'te görülmektedir.

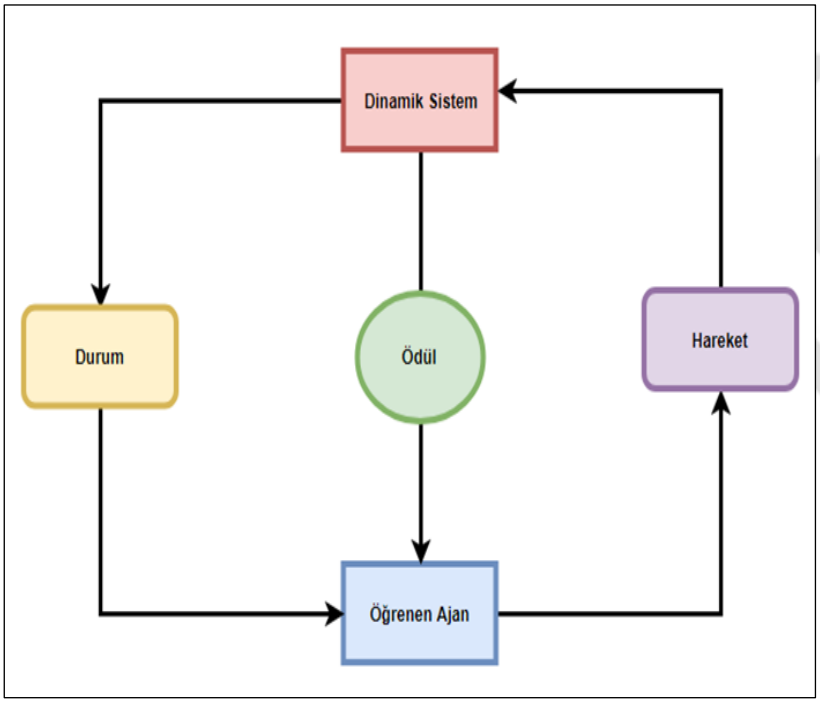


Şekil 4.4. Yarı danışmanlı öğrenme

Şekil 4.4'te görüldüğü gibi Yarı Danışmanlı Öğrenme'de etiketli veriler etiketsiz olan verileri eğitmektedir.

Takviyeli öğrenme

Takviyeli Öğrenmede sisteme girdi olarak girilen veriler sonucu elde edilen çıktılar ile hesaplanan çıktılar karşılaştırılarak sonucun doğru veya yanlış olmasına göre sisteme geri dönüş olarak ödül veya ceza verilerek sistemin öğrenmesi sağlanmaktadır. Yaygın olarak bilinen Takviyeli öğrenme yöntemi Q-Learning Metodudur [40]. Takviyeli Öğrenmeye ilişkin model Şekil 4.5'te görülmektedir.



Şekil 4.5. Takviyeli öğrenme

Şekil 4.5'te görüldüğü gibi Takviyeli Öğrenme yönteminin temeli ödül/ceza sistemi üzerine kurgulanmaktadır.

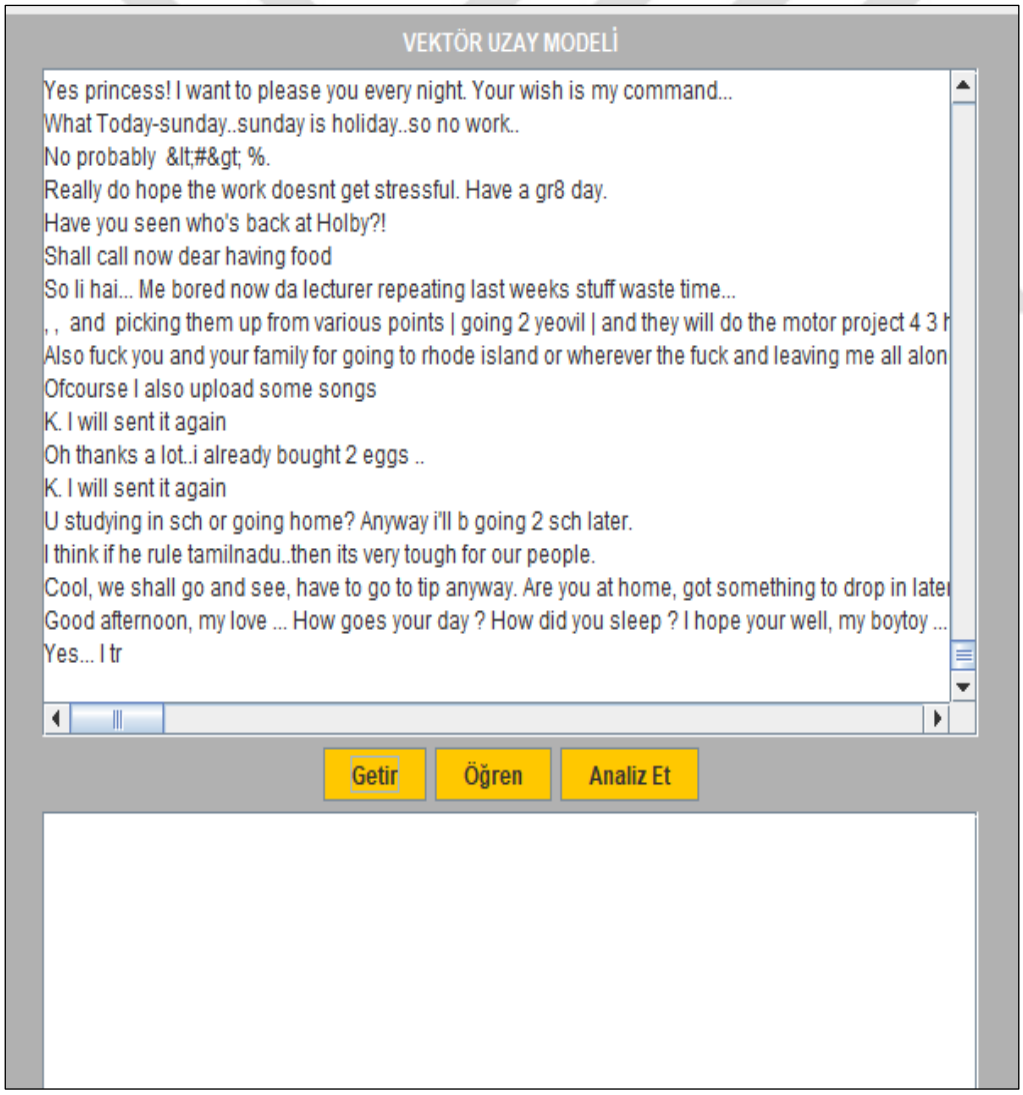
4.2.2. Sınıflandırma

Sınıflandırılması yapılmış (etiketlenmiş) veriler çeşitli algoritmalarda kullanılarak, sınıfı belli olmayan (etiketsiz) verilerin sınıflandırılması işlemidir. Makine Öğrenmesi yöntemleri içerisinde sınıflandırma için kullanılan algoritmalardan en önemlileri, Naive Bayes Sınıflayıcısı, Karar Ağaçları, Yapay Sinir Ağları, Destek Vektör Makineleri, K- En Yakın Komşuluk, Rastgele Orman gibi metotlardır.

4.3. Yöntemin Uygulanması

Çalışmada sınıflandırılması yapılacak tweet'ler için Makine Öğrenmesi modellerinden Vektör Uzay Modeli kullanılmıştır. Vektör Uzay modelinin kullanımının avantajları arasında; veri yapılarının vektörel bir uzayda doğrusal cebir kullanılarak işlenebilmesi, verilerin önemlerine göre ağırlık değeri verilerek hesaplamaların yapılabilmesi, vektörler arasında kullanılan bütün fonksiyonların metinler arasında da kullanılabilmesi (kösinüs benzerliği vb.), metnin tamamı yerine belirli bir parçası üzerinde işlem yapılabilmesi sıralanabilmektedir.

Çalışmada yapılan uygulamanın ekran görüntüsü ve elde edilen sonuçlara (çıktılara) ilişkin örnek bir kesit Şekil 4.6 ve Şekil 4.7' de görülmektedir.



Şekil 4.6. Çalışmada hazırlanan uygulamaya ait ekran görüntüsü

Şekil 4.6'da görüldüğü gibi Vektör Uzay Modeli yardımıyla eğitim için kullanılan veriseti ile sistemin eğitilmesinin ardından, uygulamaya girilen test verilerinin (veriseti veya Twitter'dan çekilen rastgele tweetler) analizi yapılarak, sisteme girilen ilgili iletilerin spam olup olmadığının sorgulaması yapılmaktadır. Şekil 4.7'de örnek test verileri görülmektedir.

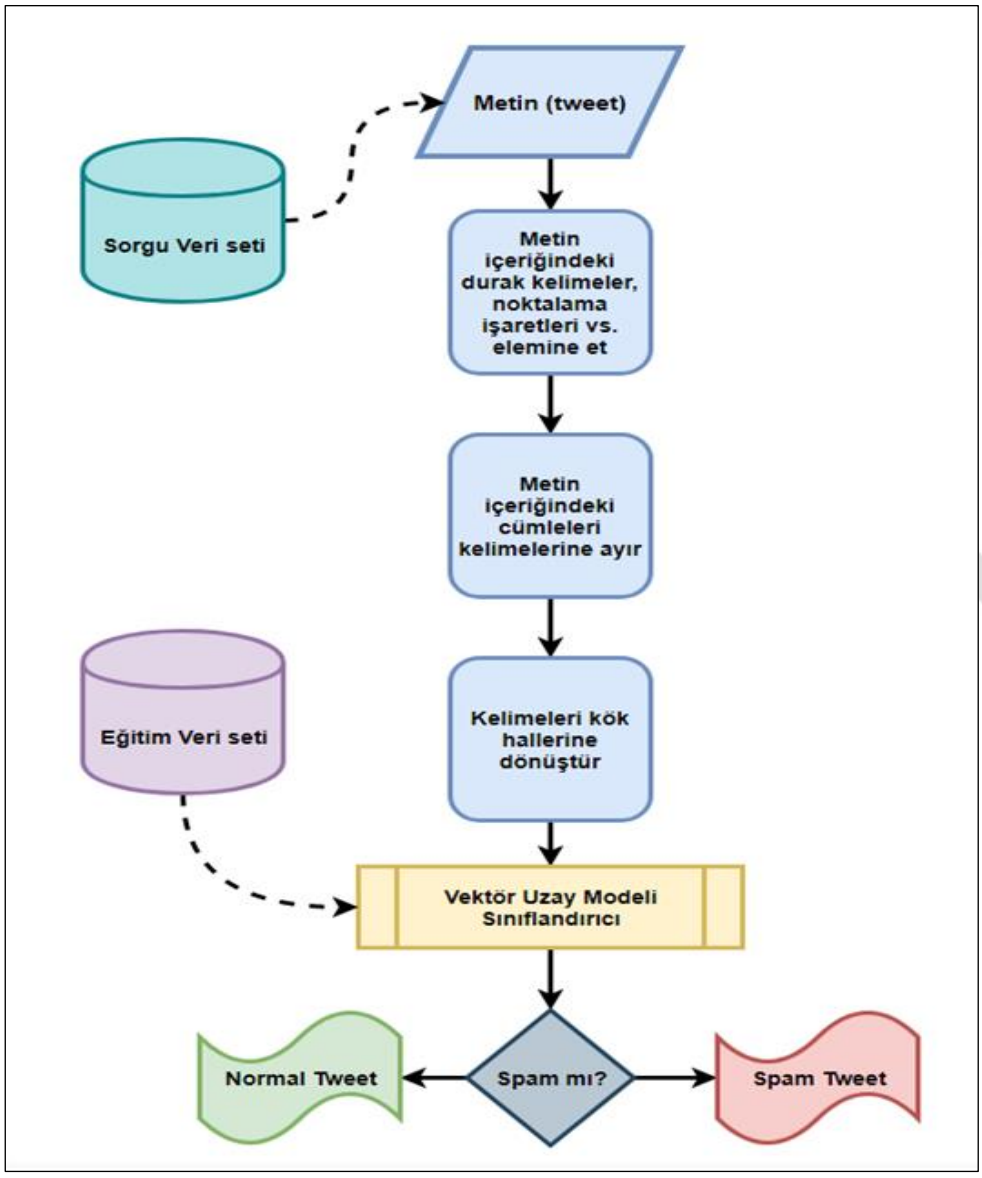
```
Spam - [Mando diao Donw in the past 2004 streaming on Download android app]
Normal - [Download Cricket Captain 2016 android game for Free n n]
Spam - [Thanks for following us The app is now live on iOS at u0026 Android at]
Spam - [The LG G4 and V10 will receive Android Nougat after all]
Spam - [ã The Cat of Happinessã ã nã iOSã]
Normal - [rhe Ebwb thig the evabs Whi tabfec to Orobido arst Te wied Di the ti I abd dhatice]
Spam - [Nokiaâ s new Android smartphone has been undraped]
Spam - [mau spotify premium come here u003e u003c only 15k for android user only]
Normal - [id oid 58d80462d27b877d8ce5998e message A new study found that overall Android users are more honest
Normal - [Y know I m still waiting on them to age some of these characters up Chibi gotta be near the same age
Spam - [low cost phones with Android are decent too]
Spam - [You can t go wrong with red Support the Global Fund with the new iPhone 7 PRODUCT RED Special Edition]
Normal - [Sent from my iPhone]
Spam - [Customize your pupper on an iPhone case today and help save another n nOnly ğŸ]
Normal - [That would bloody hurt ğŸ ³ğŸ ^]
Spam - [iMore How to make an emergency call on a locked iPhone]
Spam - [hey Ben it s been a whole week since you shouted me out still awaiting on the iPhone and visit can I g
Spam - [Impatiently waiting to spy even one post apocalypse zombie stumble around while texting on an iPhone]
Spam - [I just used for Twitter to spring clean my account Free iPhone app tnx to]
Spam - [id oid 58d80473d27b877d8ce59999 message Spend less time splitting the bill more time enjoying the mome
Normal - [Heart Balloon Sloth iPhone SE 5 5s Case]
Spam - [ğŸ ŒğŸ ¼ğŸ ğŸ ¾ğŸ Had no idea the new iPhone 7 Plus came with IMovie This has me soooo excited I mâ]
Spam - [The latest Paper Daily Thanks to]
Spam - [Thanks for following us on Twitter Why not download the app iOS at u0026 Android at]
Spam - [id oid 58d80a06d27b8788e0f709c6 message Thanks for following us join the discussion in the app iOS at
Normal - [Misfit la Vapor finalement sous Android Wear 2 0]
Normal - [id oid 58d80a11d27b8788e0f709c8 message JUAL THEME LINE OFFICIAL u0026 NON OFFICIAL KHUSUS ANDROID n
Spam - [Just discovered Dropsync for Android Using it Smart Recorder to autosync sound recordings to Dropbox]
Spam - [Internet WITHOUT Mobile DATA Available for FREE Android iPhone Simple Easy Quick Pokemon GO works]
Spam - [You re Never Over by man Glad that song exists]
Normal - [I can take good pictures on my android]
Spam - [Bass Drop Techno Create techno with 100 sounds]
Spam - [Book using Android mobile apps of u0026 get discounted deals in one click â]
Spam - [5 Android apps you shouldnâ t miss this week â Android Apps Weekly]
Spam - [id oid 58d80a40d27b8788e0f709d0 message Fix Disabled by administrator encryption policy or credential
Spam - [Ultra Security is now available on AndroNexus Store]
Normal - [id oid 58d80a59d27b8788e0f709d2 message Interesting look inside the world and how much the WH undere
Spam - [well why not put the offsets gor iPhone 7 on iOS 10 1 1 and iOS 10 1 on Yalu Dark too now]
Normal - [ã My cutie devilã ã nã iOSã]
Normal - [Annette Aragon dispelled the anomaly Scroll Eater]
Spam - [id oid 58d80b09d27b878e6096460e message Obire Mortem Download Android app u0026 Free Listen us Choice
Spam - [Acer B1 850 Build Acer AV0L0 B1 850 E 003 00 WW GEN1 5 1 Now Supported for at]
Spam - [We are very pleased to announce our new app is available now for iTunes and Android Support u0026 down
Spam - [ã Boy doll box ã ã nã iOSã]
Spam - [New Release JDCTeam jdc oneplus2 7 1 1 20170325 STABLE AOSP OnePlus2 7 1 OnePlus 2]
Normal - [Never seen such a little n niOSï¼š]
Normal - [Glad I have friends that put up with my Android in their iPhone group messageğŸ â]
Spam - [is NOW LIVE talking on Radio n nDOWNLOAD APP niTunes]
Spam - [Best Android Phone of 2017 Enter Here]
```

Şekil 4.7. Test verileri için gerçekleştirilen analiz sonuçlarına ait örnek bir kesit

Şekil 4.7'de görüldüğü gibi uygulamada kullanılan Vektör Uzay Modeli yardımıyla sisteme girilen tweet'ler analiz edilerek spam olup olmadığı belirlenmektedir.

4.3.1. Yönteme ilişkin işlem adımları

Yapılan çalışmada ilgili tweet'ler önce Vektör Uzay Modelinde kullanılmak üzere önişlem aşamasından geçirilir. Daha sonra Vektör Uzay Modeli yardımıyla ilgili tweetin spam olup olmadığı bulunarak sınıflandırılır. İlgili spam tespit analizine ilişkin işlem adımları Şekil 4.8'de görülmektedir.



Şekil 4.8. Spam analizine ilişkin gerçekleştirilen işlem adımları

Şekil 4.8'de görüldüğü gibi sorgu verisetinden veya doğrudan doğruya Twitter'dan çekilen veriler Vektör Uzay Modeli'nde kullanılmadan önce önişlem aşamasından geçirilir. Bu aşamalar, durak kelimelerin elemine edilmesi, büyük/küçük harf dönüşümü, iletilerin kelimelere ayrılması, kelimelerin köklerinin elde edilmesi şeklindedir. Daha sonra yalın hale

indirgenmiş kelime kökleri Vektör Uzay Modeli yardımıyla analiz edilmektedir. Bu analiz daha önceden oluşturulmuş eğitim verisetindeki verilerden de yararlanılarak yapılmaktadır. Başarım tespiti için kullanılan verisetleri haricinde Twitter üzerinden tweet'lerin elde edilmesi için Twitter'ın kullanıcılara sunduğu Twitter API'si kullanılmaktadır.

4.3.2. Twitter uygulama programlama arayüzü (Twitter API)

Twitter, araştırmacılara sunduğu Twitter Uygulama Programlama Arayüzü (Twitter API) sayesinde genel twitter kullanıcı hesapları üzerinde bazı veri kaynaklarına erişime izin vermektedir. Twitter API ile bir kullanıcı hesabı üzerinden erişilebilen bazı nitelikler Çizelge 4.2'de görülmektedir.

Çizelge 4.2. Twitter API ile erişilebilen bazı nitelikler

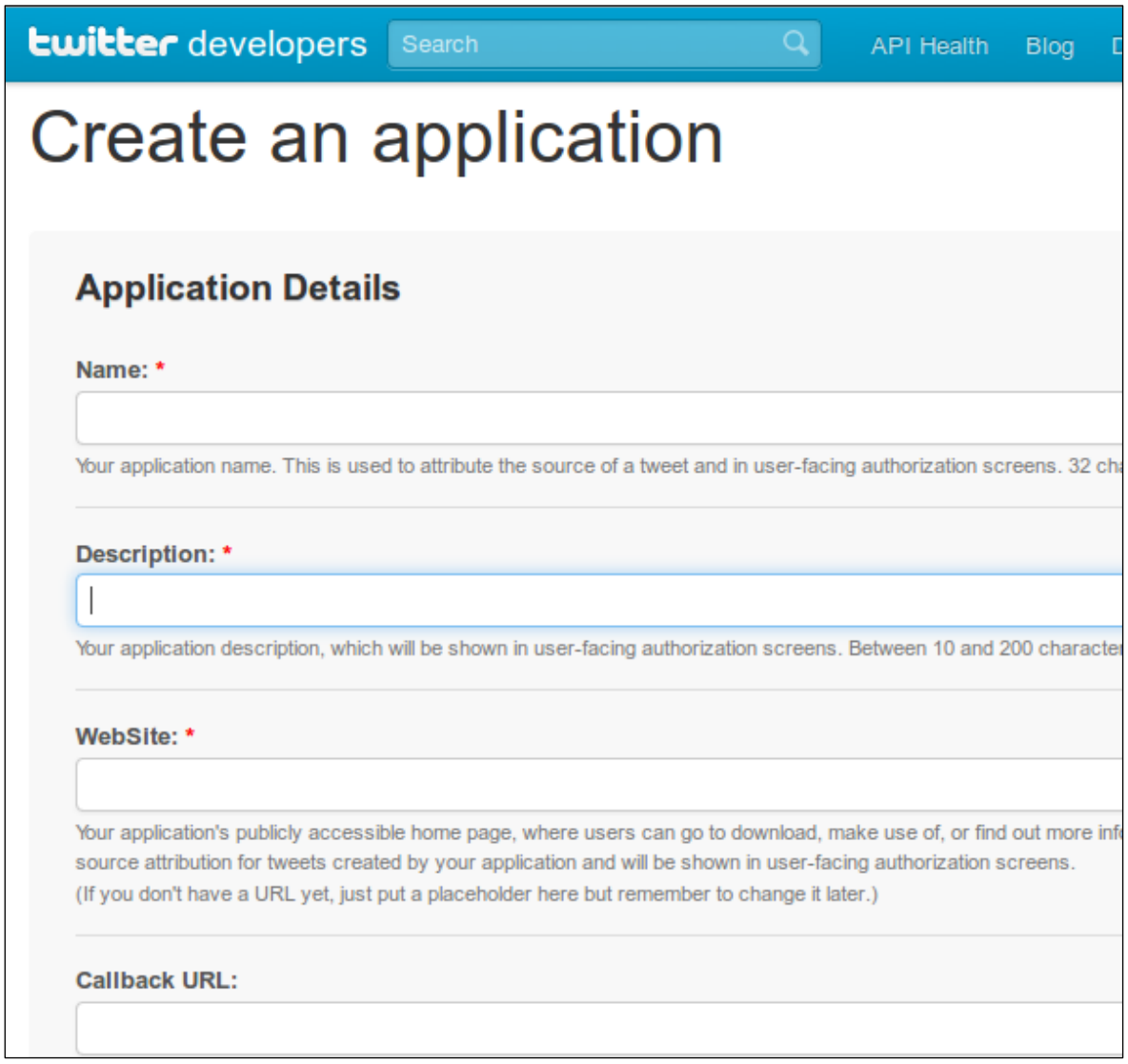
Twitter API ile Erişilebilen Bazı Nitelikler
Twitter Verisi
Tweet Status ID
Tweet İçeriği
Tweet Gönderim Tarihi
Kullanıcı Adı
Kullanıcı Tam Adı (Adı Soyadı)
Kullanıcı Takipçi Sayısı
Kullanıcı Takip Sayısı
Kullanıcı Toplam Tweet Sayısı
Kullanıcı Favori Tweet Sayısı
Kullanıcı Hesap Oluşturma Tarihi
Kullanıcının Oluşturduğu Liste Sayısı
Kullanıcı Web Sayfası
Kullanıcı Profil Açıklaması
Kullanıcı Lokasyonu
Kullanıcı Tweet URL Bilgisi

Çizelge 4.2'de görüldüğü gibi Twitter API sayesinde Twitter kullanıcı hesabı olan bir kullanıcıya ait bilgilere erişim sağlanabilmektedir.

4.3.3. Twitter verilerine erişme

Twitter verilerine erişebilmek için ilk olarak Twitter'ın program geliştiricilere sunduğu Twitter API'sine Twitter4J Java Kütüphanesi yardımıyla erişilip, belirlenen bir anahtar kelimenin (etiket) geçtiği tweet'ler elde edilmektedir. Twitter API'sine erişmek için ilk olarak Twitter uygulamasına kayıtlı bir kullanıcı hesabına ihtiyaç vardır. Ardından Twitter'a uygulama üzerinden erişilip, üzerinde işlem yapabilmeyi sağlayan Twitter'ın uygulama

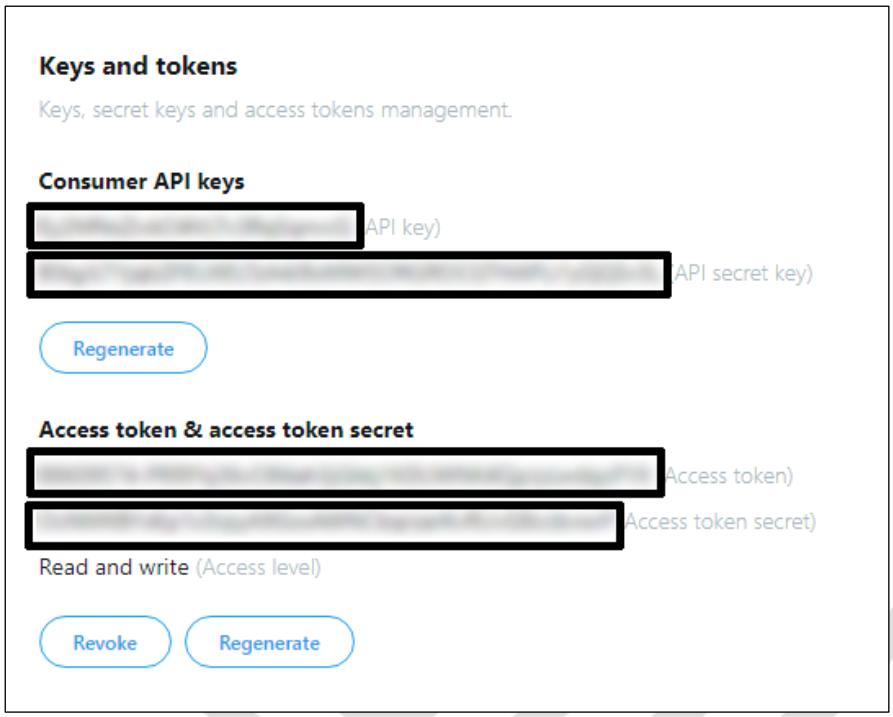
geliştiricilere sunduğu API key'lerin oluşturulması gerekmektedir. API key'leri http://apps.twitter.com/ adresi üzerinden yeni bir uygulama yaratılarak elde edilebilmektedir. Bu keyler Twitter Consumer Key (API Key) ve Consumer Secret-Access Token Key (API Secret) anahtarlarıdır. Şekil 4.9'da uygulama oluşturma ekran görüntüsü görülmektedir.



Şekil 4.9. Uygulama oluşturma ekranı

Şekil 4.9'da görüldüğü gibi Twitter üzerinde bir uygulama oluşturmak için, bir isim, ilgili uygulamaya ilişkin bir açıklama metni ve bir website ismi yazılması gerekmektedir.

İlgili uygulama oluşturulduktan sonra Twitter API keylerine erişim sağlanabilmektedir. Twitter API key'lerine ait uygulamada yer alan ekran görüntüsü Şekil 4.10'da görülmektedir.



Şekil 4.10. Twitter API keylerine ait ekran görüntüsü

Şekil 4.10'da görüldüğü gibi Twitter verilerine erişim için gerekli olan Access ve Consumer key bilgilerine uygulama oluşturma işlemleri ardından erişim sağlanabilmektedir.

Anahtar değerler Şekil 4.11.'deki Java kod parçasında görüldüğü gibidir ve twitterdan veri çekilmesi işlemlerinde kullanılmaktadır.

```
1  Twitter twitter = new TwitterFactory().getInstance();
2
3  twitter.setOAuthConsumer("2lQUlC5liCcqeaHixST6Mw8CX",
4  "o6vs68qTgX0N3tuBtZqGdOtft1IkkUIk0SFmtW92KfWwdMYUWD");
5
6  twitter.setOAuthAccessToken(new AccessToken(
7  ,"513257882-qLItvOphVpKMPEkdZoW3dAhWoW0Vd7wbRYeY4VJK",
8  "VnrtftfKGFluTRvL44D68V7TFCdUd7qNXTKp6FVmZHnSz"));
```

Şekil 4.11. Twitter'dan veri çekilmesi için kullanılan Access ve Consumer key'ler.

Şekil 4.11.'te görüldüğü gibi uygulama üzerinden elde edilen Access ve Consumer key'ler Twitter verilerine erişim için kullanılmaktadır.

API key'ler (anahtarlar) sayesinde tweet'lere erişebilmenin yanında; Tweet status id, tweet İçeriği, tweet gönderim tarihi, kullanıcı adı, kullanıcı tam adı (adı soyadı), kullanıcı takipçi sayısı, kullanıcı takip sayısı, kullanıcı toplam tweet sayısı, kullanıcı favori tweet sayısı, kullanıcı hesap oluşturma tarihi, kullanıcının oluşturduğu liste sayısı, kullanıcı web sayfası,

kullanıcı profil açıklaması, kullanıcı lokasyonu, kullanıcı tweet URL bilgisi gibi verilere de ulaşılabilmektedir.

Twitter'da herhangi bir etiketi içeren tweet'lere ulaşılabileceği gibi, kullanıcının hesabunda o anda var olan tweet'lere de ulaşılabilmektedir. Kişinin sayfasında yer alan anlık tweet'lere erişim için Şekil 4.12'de yer alan Java kod bloğu kullanılabilmektedir.

```
1  Twitter twitter = TwitterFactory.getSingleton();
2
3  List<Status> statuses = twitter.getHomeTimeline();
4
5  System.out.println("Anlık tweetler:");
6
7  for (Status status:statuses)
8  {System.out.println(status.getText());}
```

Şekil 4.12. Bir kullanıcının sayfasında yer alan anlık tweet'lere erişimi sağlayan kod bloğu

Şekil 4.12'de görüldüğü gibi "twitter.getHomeTimeline" işlevi yardımıyla bir kullanıcıya ait anlık tweet bilgilerine erişim sağlanabilmektedir.

Belirli bir etiket (hasgtag) hakkındaki tweet'leri elde etmek için ise Şekil 4.13'deki kod bloğu kullanılabilmektedir.

```
1  Query query = new Query("#etiket");
2  QueryResult result;
3  result = twitter.search(query);
4  List<Status> tweets = result.getTweets();
```

Şekil 4.13. Bir etiket (hashtag) hakkındaki tweetleri elde etmek için kullanılabilen kod bloğu

Şekil 4.13'teki Java kod bloğu sayesinde belirli bir etiket (hashtag) ile ilgili o andaki anlık tweet'lerin elde edilmesi sağlanmaktadır.

API key'ler yardımıyla ulaşılabilen twitter verilerine ait örnek bir çıktı Çizelge 4.3'te görülmektedir.

Çizelge 4.3. API keyler sayesinde erişilen örnek twitter verileri

Nitelik	Twitter İçeriği
getUser	id=14937183, name='UserName', screenName='KaygKaygi',
followersCount	309
location	'İkizce, Ordu'
description	'İster dinle ister söyle hayat bu senin şarkın ?',
friendsCount	770

Çizelge 4.3. (devam) API keyler sayesinde erişilen örnek twitter verileri

Nitelik	Twitter İçeriği
createdAt	Sat Jun 08 22:24:47 2013
statusesCount	3417
getText	#baykuş #uykucubaykuş #deneme 1 2 3.... ? @ Rize…
getAccessLevel	0
getCurrentUserRetweetId	-1
getId	835465837700055046
getInReplyToScreenName	null
getInReplyToStatusId	-1
getLang	en
getRetweetCount	9
getFavoriteCount	15
getSource	Instagram
getGeoLocation	GeoLocation{latitude=41.0449627, longitude=40.57872336}
getPlace	PlaceJSONImpl{name='Rize', streetAddress='null', countryCode='TR', id='005b1f6c10cdf2cb', country='Turkey', placeType='city'
getRateLimitStatus	null
getRetweetedStatus	null
getScopes	null
getSymbolEntities	[Ltwitter4j.SymbolEntity;@1bfb90a
getURLEntities	[Ltwitter4j.URLEntity;@29daf3
getUserMentionEntities	[Ltwitter4j.UserMentionEntity;@1660f4e
isFavorited	false
isPossiblySensitive	false
isRetweet	false
isRetweetedByMe	false
isTruncated	false

Çizelge 4.3'te görüldüğü gibi Access ve Consumer Key'ler yardımıyla bir kullanıcıya ait Twitter verileri elde edilebilmektedir.

Çalışmada içerik tabanlı spam analizi yapıldığı için Çizelge 4.3'te yer alan verilerden "getText" niteliği kullanılarak elde edilen tweet içerikleri kullanılmaktadır.

4.3.4. Verilerin önişlem aşamasından geçirilmesi

Twitter'dan elde edilen tweet içeriği sonraki işlemler için standart bir yapıya dönüştürülmesi gerekmektedir. Bu nedenle içerikteki bir takım etiketlerin temizlenmesi, sözcük karakter sıkıntılarının engellenmesi için büyük/küçük harf çevrimi yapılması, sözcüklerinin köklerinin elde edilmesi, durak sözcüklerinin (stop-words) elemine edilmesi, harf olmayan karakterlerin yerine boşluk eklenmesi gibi işlemler yapılmaktadır.

Harf olmayan karakterlerin yerine boşluk eklenmesi

Tweetlerin içeriğinde yer alan harf olmayan gereksiz karakterlerin yerine boşluk eklenmesi sağlanarak tweet'ler gereksiz karakterlerden elemine edilmektedir. Bu işlem için kullanılan kod bloğu Şekil 4.14'te görülmektedir:

```
String Text =TWEET;
Text = Text.replaceAll("htt[^\\s]+","").trim();
Text = Text.replaceAll("@\\w+\\w+|\\bRT\\b", "").trim();
Text = Text.replaceAll("\n", " ").trim();
Text = Text.replaceAll(" +", " ").trim();
Text = Text.replaceAll("\\<.*?>","").trim();
Text = Text.replaceAll("[^\\p{L}\\p{N} ]+", " ").trim();
Text = Text.toLowerCase();
Text = Text.replace(",", "");
Text = Text.replace(".", "");
Text = Text.replace(";", "");
Text = Text.replace("!", "");
Text = Text.replace("?", "");
Text = Text.replace("(", "");
Text = Text.replace(")", "");
Text = Text.replace("{", "");
Text = Text.replace("}", "");
Text = Text.replace("[", "");
Text = Text.replace("]", "");
Text = Text.replace("<", "");
Text = Text.replace(">", "");
Text = Text.replace("%", "");
Text = Text.replace("\"", "");
Text = Text.replace(":", "");
Text = Text.replace("=", "");
Text = Text.replace("-", "");
Text = Text.replaceAll("\\d", "");
return Text;
```

Şekil 4.14. Harf olmayan gereksiz karakterlerin yerine boşluk eklenmesi

Şekil 4.14'te görüldüğü gibi harf olmayan gereksiz karakterlerleri boşluk karakteri ile yer değiştirilmektedir.

Durma sözcüklerinin elemine edilmesi

Durma sözcükleri tweetlerde sıkça geçen ve tek başına bir anlam ifade etmeyen edat, bağlaçlar gibi sözcüklerdir. Bunların tweet içeriğinden temizlenmesi ayırt edicilik açısından bir farklılığa neden olmamaktadır. Hemen hemen tüm metin içeriklerinde yer aldıklarından benzerlik oluşturma veya sınıflandırma işlemleri için ayırtedici nitelik oluşturmamaktadırlar.

Uygulamada elemine edilen Türkçe durak kelimelerinin listesi Şekil 4.15'te görülmektedir.

```
public static String[] TürkçeDurakkelimeler = {
 “acaba”, “ama”, “ancak”, “artık”, “asla”, “aslında”, “az”, “bana”, “bazen”, “bazı”,
“bazıları”, “bazısı”, “belki”, “ben”, “beni”, “benim”, “beş”, “bile”, “bir”,
“birçoğu”, “birçok”, “birçokları”, “biri”, “birisi”, “birkaç”, “birkaçı”, “bir şey”,
“bir şeyi”, “biz”, “bize”, “bizi”, “bizim”, “böyle”, “böylece”, “bu”, “buna”,
“bunda”, “bundan”, “bunu”, “bunun”, “burada”, “bütün”, “çoğu”, “çoğuna”, “çoğunu”,
“çok”, “çünkü”, “da”, “daha”, “de”, “değil”, “demek”, “diğer”, “diğeri”,
“diğerleri”, “diye”, “dolayı”, “elbette”, “en”, “fakat”, “falan”, “felan”, “filan”,
“gene”, “gibi”, “hangi”, “hangisi”, “hani”, “hatta”, “hem”, “henüz”, “hep”, “hepsi”,
“hepsine”, “hepsini”, “her”, “her biri”, “herkes”, “herkese”, “herkesi”, “hiç”, “hiç
kimse”, “hiçbiri”, “hiçbirine”, “hiçbirini”, “için”, “içinde”, “ile”, “ise”, “işte”,
“kaç”, “kadar”, “kendi”, “kendine”, “kendini”, “ki”, “kim”, “kime”, “kimi”, “kimin”,
“kimisi”, “madem”, “mı”, “mi”, “mu”, “mü”, “nasıl”, “ne”, “ne kadar”, “ne zaman”,
“neden”, “nedir”, “nerde”, “nerede”, “nereden”, “nereye”, “nesi”, “neyse”, “niçin”,
“niye”, “ona”, “ondan”, “onlar”, “onlara”, “onlardan”, “onların”, “onu”, “onun”,
“orada”, “oysa”, “oysaki”, “öbürü”, “ön”, “önce”, “ötürü”, “öyle”, “sana”, “sen”,
“senden”, “seni”, “senin”, “siz”, “sizden”, “size”, “sizi”, “sizin”, “son”, “sonra”,
“şayet”, “şey”, “şimdi”, “şöyle”, “şu”, “şuna”, “şunda”, “şundan”, “şunlar”, “şunu”,
“şunun”, “tabi”, “tamam”, “tüm”, “tümü”, “üzere”, “var”, “ve”, “veya”, “veyahut”,
“ya”, “ya da”, “yani”, “yerine”, “yine”, “yoksa”, “zaten”, “zira” }
```

Şekil 4.15. Türkçede yer alan durma sözcükleri (stop words)

Şekil 4.15’teki Vektör Uzay Modeli için bir anlam ifade etmeyen (nötr özellik taşıyan) Türkçe durak kelimeler elemine edilmektedir.

Şekil 4.16’da İngilizce durak kelimelerden en önemlileri görülmektedir.

```
public static String[] EnglishStopWords = {

"without", "see", "unless", "due", "also", "must", "might", "like", ", "[", "}",
"{", "<", ">", "?", "\"", "\\", "/","will", "may", "can", "much", "every", "the",
"in", "other", "this", "the", "many", "any", "an", "or", "for", "in", "an", "an ",
"is", "a", "about", "above", "after", "again", "against", "all", "am", "an", "and",
"any", "are", "aren't", "as", "at", "be", "because", "been", "before", "being",
"below", "between", "both", "but", "by", "can't", "cannot", "could","couldn't",
"did", "didn'"most", "mustn't", "my", "myself", "no", "nor", "not", "of", "off",
"on", "once", "only", "ought", "our", "ours", "ourselves", "out", "over", "own",
"same", "shan't", "she", "she'd", "she'll", "she's", "should", "shouldn't", "so",
"some", "such", "than", "that", "that's", "their", "theirs", "them", "themselves",
"then", "there", "there's", "these", "they", "they'd", "they'll", "they're",
"they've", "this", "those", "through", "to", "too", "under", "until", "up", "very",
"was", "wasn't", "we", "we'd", "we'll", "we're", "we've", "were", "weren't", "what",
"what's", "when", "when's", "where", "where's", "which", "while", "who", "who's",
"whom", "why", "why's", "with", "won't", "would", "wouldn't", "you", "you'd",
"you'll", "you're", "you've", "your", "yours", "yourself", "yourselves", "Without",
"See", "Unless", "Due", "Also", "Must", "Might", "Like", "Will", "May", "Can",
"Much", "Every", "The", "In", "Other", "This", "The", "Many", "Any", "An", "Or",
"For", "In", "An", "An ", "Is", "A", "About", "Above", "After", "Again", "Against",
"All", "Am", "An", "And", "Any", "Are", "Aren't", "As", "At", "Be", "Because",
"Been", "Before", "Being", "Below", "Between", "Both", "But", "By", "Can't",
"Cannot", "Could", "Couldn't", "Did", "Didn't", "Do", "Does", "Doesn't", "Doing",
"Don't", "Down", "During", "Each", "Few", "For", "From", "Further", "Had", "Hadn't",
"Has", "Hasn't", "Have", "Haven't", "Having", "He", "He'd", "He'll", "He's", "Her",
"Here", "Here's", "Hers", "Herself", "Him", "Himself", "His", "How", "How's", "I ",
" I", "I'd", "I'll", "I'm", "I've", "If", "In", "Into", "Is", "Isn't", "It", "It's",
"Its", "Itself", "Let's", "Me", "More", "Most", "Mustn't", "My", "Myself", "No",
"Nor", "Not", "Of", "Off", "On", "Once", "Only", "Ought", "Our", "Ours", "Ourselves",
"Out", "Over", "Own", "Same", "Shan't", "She", "She'd", "She'll", "She's", "Should",
"Shouldn't", "So", "Some", "Such", "Than", "That", "That's", "Their", "Theirs",
"Them", "Themselves", "Then", "There", "There's", "These", "They", "They'd",
"They'll", "They're", "They've", "This", "Those", "Through", "To", "Too", "Under",
"Until", "Up", "Very", "Was", "Wasn't", "We", "We'd", "We'll", "We're", "We've",
"Were", "Weren't", "What", "What's", "When", "When's", "Where", "Where's", "Which",
"While", "Who", "Who's", "Whom", "Why", "Why's", "With", "Won't", "Would",
"Wouldn't", "You", "You'd", "You'll", "You're", "You've", "Your", "Yours",
"Yourself", "Yourselves"};t", "do", "does", "doesn't", "doing", "don't", "down",
"during", "each", "few", "for", "from", "further", "had", "hadn't", "has", "hasn't",
"have", "haven't", "having", "he", "he'd", "he'll", "he's", "her", "here", "here's",
"hers", "herself", "him", "himself", "his", "how", "how's", "i ", " i", "ı", "ı ",
"i'd", "i'll", "i'm", "i've", "if", "in", "into", "is", "isn't", "it", "it's",
"its", "itself", "let's", "me", "more"}
```

Şekil 4.16. İngilizcede yer alan durma sözcükleri (stop words)

Şekil 4.16'daki Vektör Uzay Modeli için bir anlam ifade etmeyen (nötr özellik taşıyan) İngilizce durak kelimeler elemine edilmektedir.

Sözcüklerin köklerinin elde edilmesi

Tweet içeriği kelimelere ayrılarak, daha sonraki aşamalar için standart bir hale getirilmesi için tweet içeriğindeki kelimelerin kökleri elde edilmektedir. Bu işlem için uygulamada "org.tartarus.snowball.ext.EnglishStemmer" kütüphanesi kullanılmıştır. Bu işlemin yapıldığı kod parçası Şekil 4.17'de görülmektedir.

```
1   EnglishStemmer english = new EnglishStemmer();
2
3           String [] words;
4
5           for(int m=0;m<TWEET.size();m++)
6           {
7               words = Dizi1.get(m).split("\\s+");
8               for(int n=0; n<words.length;n++)
9               {
10                  english.setCurrent(words[n]);
11                  english.stem();
12                  words[n]=english.getCurrent();
13
14                  Dizi2.add(words[n]);
15              }
16          }
```

Şekil 4.17. İngilizce sözcüklerin köklerine indirgenmesi için kullanılan kod bloğu

Şekil 4.17.'deki kod bloğunda görüldüğü gibi tweet içeriğindeki sözcüklerin hepsi teker teker köklerine ayrılarak bir diziye atılmaktadır.

Kökleri elde edilmiş bazı İngilizce kelimeler Şekil 4.18'de görülmektedir.

Kelime	Kökü	Kelime	Kökü
consign	consign	knack	knack
consigned	consign	knackeries	knackeri
consigning	consign	knacks	knack
consignment	consign	knag	knag
consist	consist	knave	knave
consisted	consist	knaves	knave
consistency	consist	knavish	knavish
consistent	consist	kneaded	knead
consistently	consist	kneading	knead
consisting	consist	knee	knee
consists	consist	kneel	kneel
consolation	consol	kneeled	kneel
consolations	consol	kneeling	kneel
consolatory	consolatori	kneels	kneel
console	consol	knees	knee
consoled	consol	knell	knell
consoles	consol	knelt	knelt
consolidate	consolid	knew	knew
consolidated	consolid	knick	knick
consolidating	consolid	knif	knif
consoling	consol	knife	knife
consolingly	consol	knight	knight
consols	consol	knightly	knight
consonant	conson	knights	knight
consort	consort	knit	knit
consorted	consort	knits	knit

Şekil 4.18. Kökleri elde edilmiş örnek İngilizce kelimeler

Şekil 4.18'de görüldüğü gibi Vektör Uzay modelinde kullanılmak üzere kelimeler köklerine indirgenerek standart hale getirilmektedir.

Türkçe içerikli kelimelerin köklerinin elde edilmesinde Zemberek API'si kullanılmıştır. Zemberek, Türk dilleri için kullanılan açık kaynak bir Doğal Dil İşleme (DDİ) kütüphanesidir [41]. Zemberek yardımı ile kelimelerin kök halleri elde edilebilmektedir. Zemberek içerisinde, Türkçedeki kelimeler ve bu kelimelerin köklerini barındırabildiği için yanlış yazılan kelimeleri +-1 harf hatasını düzeltebilmektedir.

Türkçedeki tüm kök ve gövdeler Zemberek sözlüğü içerisine yerleştirilmiştir ayrıca gövdelerde veya kökte meydana gelebilecek her tür ses değişimi de Zemberek'te yer almaktadır. Kelime incelenirken karakter karakter ilerlenerek Zemberek içerisinde aranmakta ve bir kelimenin olası kök veya gövdesine erişilince eklerin ayrıştırılması gerçekleştirilmektedir.

Latin harfleri kullanarak yazılmış Türkçe öğeleri tekrar Türkçe'ye özel harflere dönüştürme işlemi için ise Turkish Deasciifier API'si kullanılmıştır. Bu sayede Türkçe karakter içermeyen bir klavye ile yazılmış bazı karakterlerlerin Türkçe'ye özel harflere (i>ı, g->ğ, u->ü, s->ş, c-ç, o->ö) dönüşümü yapılabilmektedir. Örneğin: "Hadi bir masal uyduralim, icinde mutlu, doygun, telassiz durdugumuz." yazısı, deasciifying işlemi sonrasında; "Hadi bir masal uyduralım, içinde mutlu, doygun, telaşsız durduğumuz." şeklinde bir dönüşüme tabii olmaktadır [42].

Şekil 4.19'da Türkçe kelimelerin kök hallerinin elde edilişine ait kod parçası görülmektedir.

```
for(int i=0;i<KelimeDizisi.size();i++)
{
    Zemberek zemberek_3= new Zemberek(new TurkiyeTurkcesi());

    if(zemberek_3.kelimeDenetle(KelimeDizisi.get(i)))
    {
    kok=zemberek_3.kelimeCozumle(KelimeDizisi.get(i))[0].kok().icerik();

    KökDizisi.add(kok);
    }
        //***//
}
```

Şekil 4.19. Türkçe kelimelerin kök hallerinin elde edilmesi

Şekil 4.19'daki kod bloğunda görüldüğü gibi kelimeler Zemberek API'si yardımıyla köklerine indirgenmektedir.

Çalışmada yer alan spam ve spam olmayan Türkçe içerikli verisetlerine ait örnek bir kesit Şekil 4.20'de ve bu veriseti kesitinde yer alan içeriklerinin gereksiz içerikten temizlenerek, içeriğinde yer alan ifadelere ait kelimelerin Zemberek API'si ile kök hallerine indirgenmiş halleri Şekil 4.21'de görülmektedir.

KIGILI'dan son sans CardFinans'a ozel 7 taksitle! Gomlek,pantalon ve triko 39TL, mont-kaban 99TL, takim elb. 199TL!Inanilmaz fiyatlar ekstra hediye cekleriyle! 444cicek.com da Avealilara tum urunlerde %20 indirim. CICEK yaz, 5060a gonder, sifren cebine gelsin. avea.com.tr/avantajavea Aveadan SUPER bir Muzik Paketi! MAXI yaz, 5555e gonder, Maxi Muzikindir Paketi ile 150 yerli 50 Yabanci sarkiyi ayda sadece 5,99 TLye cebine indir! Kis sezonunun beklenen son indirimiSizleri magazalarimiza bekliyoruzwww.roman.com.tr En yakin Denizbank subesine gelin sadece Avealilara ozel hem %0,77den baslayan oranlarla 77 ay vadeli kamu kredisi kullanin hem de 40TL fatura indirimi kazanin! Beklenen gun geldi, tum sezon urunlerinde ETIKETIN YARISI kampanyasi sizleri Relax Mode magazalarinda bekliyor. Maximum Kart'la 1-10 Subatta 1000TL alisveris yapin,12-13-14 Subatta kampanyali sektorlerde yapacaginiz alisverislerden %10MaxiPuan kazanin!Bilgi:maximum.com.tr Simdi e-faturaya gecin,Toyota Prius kazanma sansi yakalayin.E-faturaya gecmek icin e-posta adresinizi SMS ile 3008'e gonderebilirsiniz.Detaylar: www.avea.com.tr Ayda 29TLye AveaKamulularla SINIRSIZ, Avealilarla 3000dk, heryone 300dk konusabileceginiz KAMU300 PLUS Tarifesine gecmek icin 300PLUS yazip 2010a gonderin. Etiketin Yarisi Indirimi Baslamadan Once, Urunlerimizi Oncelikli Satin Almak Icin, Siz Ozel Musterilerimizi Bugun ve Yarin Magazalarimiza Bekliyoruz. Sadece 1,5 TL'ye gunluk internet cebinizde!GUN yazip, 5555 e gonderin, 1 gun boyunca 100 MB internet ile cepten internete baglanin! YARIN(20 OCAK) VICHY-LA ROCHE UZMANININ ECZANEMIZDE YAPACAGI UCRETSIZ CILT VE SAC ANALIZ GUNUNE DAVETLISINIZ..BU OZEL GUNU KACIRMAYIN...3209693 23 Subat'a kadar Is Bankasi'ndan TTNET faturaniz icin talimat verin, cekilis ile Golf marka araba, Paris seyahati ya da Nokia Booklet kazanin!4440202 Çanakkale Atasay'da %25'e varan Altinci Gün indirim firsatlari,Dünya Kadinlar Günü'ne özel 5-8 Mart tarihleri arasinda uygulanacaktir.Detaylar 0286 213 20 97 Stefanel'de Dunya Kadinlar Gunu'ne ozel, sadece CardFinans sahiplerine kurk grubunda %20 Indirim ve 7 Taksit firsati! Son gun 8 Mart!]

Şekil 4.20. Uygulamada yer alan Türkçe içerikli spam verisetine ait bir kesit

Şekil 4.20'de görüldüğü gibi Türkçe içerikli ifadelerden oluşan bir spam veriseti text dosyası olarak oluşturulmuştur. Şekil 4.21'de bu verisetinde yer alan içerik gereksiz öğelerden arındırılarak elde edilen kelimelerin Zemberek API'si yardımıyla kök hallerine indirgenmiş şekilleri yer almaktadır.

[dan, son, şans, özel, taksit, gömlek, ve, triko, mont, kaban, takım, inan, fiyatla, ekstra, hediye, çek, da, tüm, ürün, indir, çiçek, yaz, gönder, cebin, gel, süper, bir, müzik, paket, ile, yerli, yabancı, şarkı, ay, sadece, kış, sezon, bekle, mağaza, roman, en, yakın, gelin, hem, de, başla, oran, vade, kamu, kredi, kullan, fatura, kazan, gün, etiket, kampanya, siz, kart, şubat, yapı, sektör, yap, bilgi, sim, geçin, yakala, geç, posta, detay, sinir, tarife, gönderi, yarış, önce, satın, al, için, bugün, yarın, tl, günlük, cep, boyun bağla, yar, ocak, eczane, ücret, saç, analiz, günü, davet, bu, kadar, iş, banka, talimat, veri, golf, marka, araba, seyahat, ya, varan, fırsat, kadın, ne, mart, tarih, ara, uygula, dünya, kürk, grup, indirim, son, gün, mart , fark, sefer, akaryakıt, alım, kuru, temizle, alternatif, ceket, veya, elbise, biri, dönüş, muhteşem, ol, ayı, dön, bilet, ayrıntı, kısa, karı, seçil, geçer, kaçır, adet, üzeri, haber, dakika, toplam, park, ön, dahil, yerin, hemen, gir, eskişehir, aylık, dans, kurs, ahmet, şerif, in, avuç, kelebek, set, saat, kur, ingilizce, almanca, eğitim, say, hazır, giyim, büyük, devir, üstelik, ilk, çar, yararlan, bedava, mevcut, harca, taşı, ekstre, söz, masraf, faiz, nisan, petrol, ofis, mayıs, mavi, yeni, sen, kulüp, üye, tamamen, servis, festival, ta, aksesuar, kozmetik, optik, elektronik, internet, daha, ucuz, keyfi, doy, her, yön, faydalan, yazın, durum, bekir, üstat, adana, ayran, çeşit, salata, lezzet, çeki, mobilya, baş, üzere, süre, otomatik, ödeme, seçenek, havale, parola, garanti, ziyaret, edin, merkezi, hitabet, meşhur, konya, kardeş, et, ekmek, sis]

Şekil 4.21. Türkçe spam verisetinde yer alan kelimelerin köklerine indirgenmiş halleri

Şekil 4.21'de görüldüğü gibi Zemberek API'si yardımıyla ilgili Türkçe verisetinde yer alan içerikler gereksiz ifadelerden arındırılarak elde edilen kelimeler kök hallerine indirgenmişlerdir. Şekil 4.22'de Türkçe içerikli spam olmayan veriler içeren verisetine ilişkin örnek bir kesit görülmektedir. Şekil 4.23'te ise bu verisetinin içeriğinde yer alan içeriğin gereksiz öğelerden arındırılarak elde edilen kelimelerin köklerine indirgenmiş halleri yer almaktadır.

oldu tamam bu sefer Bilmiyorum onu ya **5992 nolu Kredi Karti Ekstre Borcunuz 1,401.67 TL Asgari Odeme Tutari 281.00 TL ve Son Odeme Tarihi 06.06.2011 dir. hacı yarın sizdeyim yemekte ona göre hic mesj fln atmıyosunn .. SN.CAFER KAYA ARTIBILET UYELIK SIFRENIZ :1809 WWW.ARTIBILET.COM-YOLCULUKTAN DAHA FAZLASI anne ben yrn size staj ile ilgili bi belge göndercem,onu sizin telekoma ulaştırmanız gerkio.,cok öptümm beybimmmmm:))) Sari sekerlm benim iyiki dogmus yapimda emegi gecen herkese sayglar:)) En erken kaÇta gelirsin Tamam haber et madem müsait olunca. cabuk gel kahvalti yapalim yemek hazırmı ?? 10 dakikaya çıkıcam canım evden Işin yoksa langırtlı kısma uğrar mısın SN ALPER KURSAT UYSAL, PNR: SBAAST 25MAY 22:55 TK7120 UCUSUNUZ ICIN ONLINE CHECK-IN ISLEMINIZ YAPILMISTIR. BU SADECE BILGI AMACLI BIR MESAJDIR. BINIS KARTI YERINE GECMEZ. abi işim var o saatte tam Bu sefer eminim :) aynen kuzu benım acelem var sora konusuruz yıne bendede kontor yok haci :) Sizi arayan numaralar: "05351234567" (03.06,13:18)(3) Bu mesaj ucretsizdir. Guray bizim postalama isi ogleden sonraya kalacak sanirm.ddigerlerine ulasinca sana haber verirm biz napacagimizi 0433232685 buydu Hadi ya tmm :S benim bir isim cikti Kanka Sıla ben Deniz biraz dışarı çıkacaz sokak festivaline falan değil ama ihtiyaçlarımızı falan alcaz. esbayda maç var 8-9 ben faruktayım sende tarih notları var diye bakmadım hiç Yurda ugrayıp aldıklarımızı bırakıp öyle gitcez abi. neredesin kantine gel. ya cnm dün aydan mesaj attı sürekli bursaya çağırıyo müsaitsen haftasonu gidelimmi ben yatiyorum hadi Abi şimdi kargoya geldik, paketin ağırlığı fazlaymış, transkriptleri yollamıycaz cuma orda olurmuş belgeler bilgisayarı getir mutlaka kanka derse kalmak için 5-6 gibi gelirim ben. Hangover dayız gel Posterim bitti şimdi Denizle gidip çıktı alıp Yunus Emre kampüsüne götürcez kanka. Dostum vahit imza atti atmis bizim yerimize oryantasyonun sonunda yoklama yapip imzalari silmisler:(fark etmez sende kalsin anahtar iki dakaya geliyorum ben cıkıyorum evden İstatistik sınavında en son hangi konu çıkıcak biliyormusun? kanatlıda buluşuruz Abi gunaydin.kac gbi gecioz okula? almanca. GençTarifeli! sadece 10 tl ye 30 gün boyunca her yöne mesajlaşacağın tam 5000 sms icin bu mesajı EVET yazıp cevapla,fırsatı kaçırma! Neyse Emo gelmiyor Orçunda cevap atmadı. Akşam haberleşiriz yine gelirsin sen :) . sus kiz gezdin gezdin askimmis.. 1. ve 2. soru tamam gibi 3. soruda sıkıntı var tatlım ya ogelden sonraki derse giriyo msun nasilsin Kanka gelirken 2 tane buz parmak al bana daaaa :) tamamdır. Kanka oryantasyon sinema anadoludaymış. Cnm bgn geldim ben kirsehrden. Yarin bulusalim müsaitsn olur mu? Kntör yoksa faceden msj at yatmadan bakarım tamam.öpt canm.. hayırlı akşamlar ne yapıyıyorsunuz ablalarım. nasılsınız? yiğenim ne yapıyor? okula devam etsin düzenli kereta:=) annenler haftasonu geliyorlardı dimi? la get kuzum misafir var şimdi atamıcam]

Şekil 4.22. Uygulamada yer alan Türkçe içerikli spam olmayan verisetine ait bir kesit

Şekil 4.22'de görüldüğü gibi Türkçe içerikli ifadelerden oluşan bir spam olmayan veriseti text dosyası olarak oluşturulmuştur. Şekil 4.23'te bu verisetinde yer alan kelimelerin Zemberek API'si yardımıyla kök hallerine indirgenmiş şekilleri yer almaktadır.

[ol, tamam, bu, sefer, onu, ya, kredi, kart, ekstre, borç, tl, asgari, ödem, tutar, tl, ve, son, ödem, tarihi, hac, yar, siz, yemek, ona, re, cafer, kaya, üye, yolcu, daha, anne, ben, siz, staj, ile, ilgi, belge, onu, siz, ula, çok, sarı, şeker, ben, doğ, yapı, geçen, herkes, en, erken, ta, gelir, tamam, haber, et, madem, ol, çabuk, gel, kahvaltı, yap, yemek, haz, dakika, cam, can, m, ev, yoksa, alper, kürşat, uysal, uçuş, için, in, işlem, bu, sadece, bilgi, bir, yerin, geç, var, o, saat, tam, bu, sefer, emin, aynen, kuzu, ben, m, acele, var, sor, konuş, ne, kontör, yok, hacı, ara, numarala, bu, mesaj, ücret, güray, biz, postala, öğle, sonra, kal, ulaş, sen, haber, biz, buy, hadi, ya, ben, bir, isim, la, ben, deniz, biraz, ar, sokak, festival, falan, ama, falan, var, ben, m, sen, tarih, not, var, diye, m, yurt, nere, kantin, gel, ya, ay, mesaj, ben, yat, hadi, imdi, kargo, gel, paket, cuma, belgele, bilgisayar, getir, mutlaka, ders, kal, gibi, gelir, ben, gel, poster, bit, imdi, deniz, git, al, yunus, emre, dost, vahit, imza, at, at, biz, yer, son, yokla, yap, imza, fark, et, sen, kal, anahtar, iki, gel, ben, yorum, ev, en, son, hangi, konu, da, buluş, günaydın, kaç, okul, al, gen, tarife, sadece, ye, boyun, her, ne, tam, bu, mesaj, evet, yaz, cevapla, ney, gel, un, cevap, aka, yine, gelir, sen, sus, gez, gez, aşk, ve, soru, tamam, gibi, soru, var, m, ya, sonra, ders, nasıl, gelir, tane, buz, parmak, al, ben, sinema, gel, ben, yarın, buluş, ol, mu, yoksa, at, yat, bak, m, tamam, hay, ne, yap, abla, m, nas, ne, yap, yor, okul, devam, et, dimi, la, kuzu, misafir, var, şimdi, ata]

Şekil 4.23. Türkçe spam olmayan verisetindeki kelimelerin köklerine indirgenmiş halleri

Şekil 4.23'te görüldüğü gibi Zemberek API'si yardımıyla ilgili Türkçe verisetinde yer alan kelimeler kök hallerine indirgenmişlerdir.

Gereksiz içerikten arındırılıp kök halleri elde edilmiş (önişlem aşamasından geçirilmiş) kelimeler Vektör Uzay modeline giriş olarak verilmek üzere hazır hale gelmiş bulunmaktadır.

4.3.5. Vektör uzay modeli

Vektör Uzay Modeli'nde belgeler, içerisinde yer alan ve terim olarak adlandırılan öğelere ağırlık değerleri verilerek çok boyutlu uzayda matematiksel olarak ifade edilmektedirler.

Sözcüklerin vektörel olarak ifadelendirilmesi

Metin şeklindeki verilerin bir sınıflandırmaya tabi tutulması ve üzerinde işlem yapılabilmesi için sözcükler ağırlıklandırılarak bir gösterim şekli almakta ve üzerinde işlem yapılabilir şekle dönüştürülmektedir. Sözcük ağırlıklandırma bir nevi sözcüklerin metin içerisindeki etki değerlerinin belirlenmesi işlemidir. Kök haline dönüştürülmüş sözcüklerin metin içerisinde yer alma durumlarına göre değeri hesaplanmaktadır.

Bit ağırlıklandırma

Binary veya boolean ağırlıklandırma olarak da bilinir. İlgili sözcük bir belgede yer alıyorsa "1" yer almıyorsa "0" değerini alır. Bir sözcüğün birden fazla bir belgede yer alması değerini değiştirmez, eşit ağırlıkta kabul edilir.

Sözcük frekansı ağırlıklandırma (tf)

Sözcük Frekansı hesabında, bit ağırlıklandırmadan farklı olarak bir sözcüğün bir belgede ne kadar sayıda geçtiği de işleme katılmaktadır. Bu sayede bir sözcüğün belgede geçme sayısı ne kadar fazla olursa o sözcük o belge için o denli değerlidir anlamı çıkarılmaktadır.

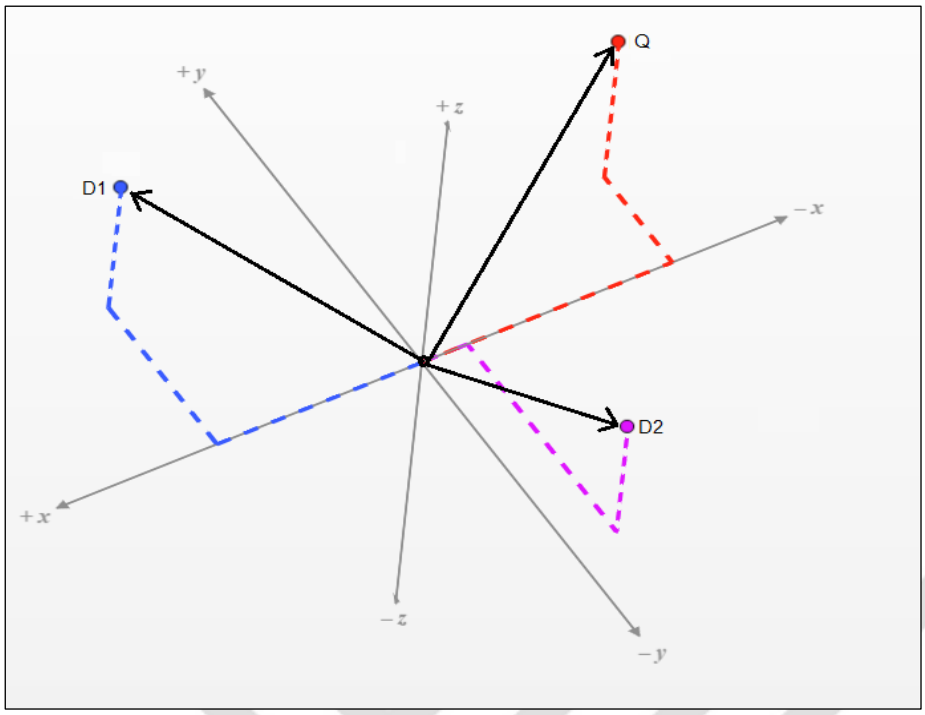
Ters belge ağırlıklandırma (idf)

Sözcük ve bit ağırlıklandırmadan farklı olarak bir sözcüğün bir belgede yer almasının yanında diğer belgelerde yer alma sayısı da Ters Belge Ağırlıklandırma için önemlidir. Bir sözcüğün birden fazla belgede yer alması belirleyicilik değerini azaltmaktadır. Bir sözcük bir belgede yer alırken diğer belgelerde hiç geçmemesi o sözcüğün değerini yani belirleyiciliğini artırmaktadır.

Sözcük frekansı-ters belge ağırlıklandırma (tf-idf)

Bu ağırlıklandırma yönteminde, Ters Belge Ağırlıklandırmadan farklı olarak sözcüğün bir belgede geçmesinin yanı sıra ne sıklıkta geçtiğinin de önemi vardır. Bu anlamda; farklı belgelerde sık yer almayan sözcükler, sık yer alanlara göre daha belirleyici değere sahiptir. Bir sözcüğün bir belgede sık görülmesi, az görülmesinden daha belirleyici değere sahiptir şeklinde yorumlama yapılabilmektedir.

Şekil 4.20'da Vektör Uzay Modelinde matematiksel olarak ifade edilmiş D_1 ve D_2 eğitim veri belgesi ile Q olarak adlandırılmış sorgu verisi örneği ve bu belgelerin vektör uzayında temsil ediliş biçimleri görülmektedir.



Şekil 4.24. D_1, D_2 ve Q örnek belgelerinin vektör uzayındaki konumları

Şekil 4.24'te görüldüğü gibi D_1 ve D_2, rastgele terimlerden oluşturulmuş eğitim veri sınıfına ait vektörleri, Q ise Vektör Uzay Modeli kullanılarak kendisine en yakın eğitim veri sınıfına (D_1 veya D_2) dâhil edilmek üzere rastgele seçilmiş sorgu verisine ait vektörü temsil etmektedir.

Terimler belge içerisindeki ayırt edicilik seviyelerine göre 0 ile 1 arasında ağırlıklandırılır. Ağırlık değerlerinin hesabında, Terim Frekansı-Ters Doküman Frekansı Ağırlıklandırma (TF-IDF)'dan yararlanılmaktadır. Vektör Uzay Modelinde iki belge arasındaki benzerlik bulunurken kosinüs benzerlik hesabı kullanılmaktadır [43].

Terimlerin belge içerisindeki ağırlıklık değerlerinin hesaplanması için Eş. 4.1 kullanılmaktadır. w_{ik}: D_i (i'inci belge) belgesindeki T_k (k'ıncı terim) teriminin ağırlık değerini, tf_{ik}: T_k teriminin D_i belgesinde yer alma sayısını (terim frekansı(TF)), N: Belge sayısını, v: Bir belgedeki terim sayısını, n_k: T_k teriminin en az bir defa yer aldığı belge sayısını, $\log\left(\frac{N}{n_k}\right)$: Ters belge frekansını (IDF)'dır [44].

$$w_{ik} = \frac{tf_{ik} \cdot \log\left(\frac{N}{n_k}\right)}{\sqrt{\sum_{j=1}^{v}(tf_{ij})^2 \cdot \left(\log\left(\frac{N}{n_j}\right)\right)^2}} \tag{4.1}$$

Eğitim belgesindeki terimlerin ağırlık değerleri kümesi D_i= (w_{i1}, w_{i2}, w_{i3}…w_{iv}) ve sorgu belgesinde yer alan terimlerin ağırlık kümesi Q_j= (w_{j1}, w_{j2}, w_{j3}…w_{jv}) olmak üzere D_i ile Q_j belgeleri arasındaki benzerlik hesabı için Eş. 4.2 kullanılmaktadır. Bu hesaplamaya kosinüs benzerlik hesabı olarak adlandırılmaktadır. İki belge arasındaki açının kosinüs değerine göre benzerlik oranı hesaplanmaktadır.

$$Sim(Q_j, D_i) = \sum_{k=1}^{v} w_{jk}.w_{ik} \quad (4.2)$$

Terim Frekansı (TF), kelimenin bir belgede geçme sayısının, ilgili belgede yer alan toplam kelime sayısına oranı ile hesaplanmaktadır. Terim frekansı hesaplaması, eğitim ve sorgu belgelerindeki her bir kelime için yapılmaktadır.

Ters belge frekansı (IDF), sistemde yer alan belgelerin sayısının (N), bir kelimenin en az bir defa yer aldığı belge sayısına (n_k) oranının logaritması ile hesaplanmaktadır. Bu değer, tüm belgeler içerisinde yer alan ve ayırt ediciliği fazla olan kelimeler ile belgelerdeki iletilerin içeriğinde sıklıkla yer alıp ayırt ediciliği fazla olmayan kelimelerin tespit edilmesinde kullanılmaktadır [45].

Bir kelimenin bir belgedeki ağırlık değerleri (w_{ik}), bu kelime için hesaplanmış TF*IDF değerinin, belgede yer alan her bir kelime için hesaplanan TF*IDF değerlerinin karelerinin toplamından elde edilen değerin karekökü ile oranı ile hesaplanmaktadır.

Sorgu belgelerinin (Q_j) eğitim belgelerine (D_i) olan kosinüs benzerlik değeri, sorgu belgelerindeki iletilerin içeriğinde yer alan her bir kelimenin ağırlık değeri ile eğitim belgelerindeki iletilerin içeriğindeki her bir kelimenin ağırlık değerinin çarpımlarından elde edilen değerlerin toplamı ile hesaplanmaktadır. Bir iletinin spam ileti olup olmadığı, bu iletinin eğitim belgelerinde yer alan iletiler ile olan benzerlik değerine göre tespit edilmektedir. Kosinüs benzerlik değerinin yüksekliği iki belge arasındaki benzerliğin fazla olduğu anlamına gelmektedir.

Çizelge 4.4. D_1, D_2 ve Q örnek belge içerikleri

D_1 (spam içeren belge örneği)	**D_2 (spam olmayan belge örneği)**	**Q (sorgu belgesi)**
#click #win #here #click #buying	#click #going #car #here #goes #bus	#click #here #open #door #win

Çizelge 4.4'te örnek olarak, D_1 ve D_2 sınıflarına ait veri kümeleri ile bu sınıflardan kendisine en benzer olana dâhil edilmek üzere Q test veri kümesi belirlenmiştir.

Çizelge 4.5. Ön işlemden geçirilmiş ve kelimelerine ayrılmış D_1, D_2 ve Q belgeleri

D_1	D_2	Q
click	click	click
win	go	here
here	car	open
click	here	door
buy	go	win
-	bus	-

Çizelge 4.5'te görüldüğü gibi D_1, D_2 ve Q belgeleri ön işlemden geçirilmiş, gereksiz noktalama işaretleri kaldırılarak ilgili ifadeler kelimelerine ve kök hallerine indirgenmiştir.

Çizelge 4.6. Terim frekanslarının hesaplanması

Terim	Terim Frekansı (tf_i)		
	Q	D_1	D_2
click	0.2	0.4	0.16
win	0.2	0.2	0
here	0.2	0.2	0.16
buy	0	0.2	0
home	0	0	0.33
car	0	0	0.16
bus	0	0	0.16

Çizelge 4.6.'da D_1, D_2 ve Q belgelerine ait terimlere ilişkin hesaplanan terim frekans değerleri görülmektedir. Vektör Uzay Modeli'nde, bir terimin bir belge içerisinde yer alma sayısının, ilgili belgede yer alan tüm terimlerin sayısına oranı terim frekansı (tf) olarak ifade edilmektedir.

Çizelge 4.7. Terim ağırlıklarının hsesaplanması

Belge Frekansı	**Belge Sayısı/Belge Frekansı**	**Ters Belge Frekansı**	**Ağırlık Değeri ($w_i = tf_i * idf_i$)**		
df_i	D/df_i	idf_i	Q	D_1	D_2
3	0.66	0.18	0.036	0.072	0.03
1	2	0.3	0.06	0.06	0
2	1	0	0	0	0
1	2	0.3	0	0.06	0
2	1	0	0	0	0
1	2	0.3	0	0	0.05
1	2	0.3	0	0	0.05

Çizelge 4.7'de görüldüğü gibi ön işlem aşamasından geçirilmiş terimlerden, D_1 ve D_2 belgelerinde ortak olarak yer alanların tespit edilmesinin ardından; terim frekansı, belge frekansı, ters belge frekansı ve bu değerlerden yararlanılarak her bir terime ait ağırlık değerleri hesaplanmıştır. Bir terimin kaç adet belgede yer aldığı bilgisi belge frekansı (df) ile ifade edilir. Ters belge frekansı (idf), modelde yer alan toplam belge sayısının (D), belge frekansına (df) oranının logaritması alınarak elde edilir. Her bir terimin, bir belge içerisindeki ağırlık değeri (w) ise ilgili terime ait terim frekansı (tf) ile ters belge frekansının (idf) çarpımı ile hesaplanır.

Terimlerin ağırlık değerlerinin hesaplanmasının ardından, vektörler arasındaki mesafeler (D_1,D_2 ile Q) hesaplanarak sorgu verisi vektörünün hangi eğitim verisi vektörüne daha çok benzediği belirlenir. İlgili hesaplama için bu çalışmada Kosinüs Benzerliği yöntemi kullanılmıştır. Bu yönteme göre vektör uzayında yer alan eğitim verisi vektörleri ile sorgu verisi vektörü arasındaki açının kosinüs değeri hesaplanarak, bu vektörlerin birbirlerine olan yakınlık değerleri elde edilir. Bu yakınlık değerine göre sorgu verisi vektörünün en çok benzerlik gösterdiği eğitim verisi sınıfı belirlenmiş olur.

İki vektör arasındaki açının kosinüsü Eş. 4.3 ile hesaplanmaktadır:

$$\cos(Di,Q) = D_i \bullet Q / |D_i||Q| \quad (4.3)$$

Eş. 4.3'de $|D_i|$ ve $|Q|$, belgelerin içeriğindeki terimlerin sahip oldukları ağırlık değerlerinin (w_i) karelerinin toplamının karekökü alınarak hesaplanır.

$|D_1| = 0.1112$,

$|D_2| = 0.0768$,

$|Q| = 0.0699$ olarak elde edilir.

İlgili hesaplamalar sonucunda elde edilen değerler ışığında;

$|D_1||Q| = 0.0077$,

$|D_2||Q| = 0.0053$ olarak elde edilir.

$D_i \bullet Q$ değeri; belgelerde yer alan her bir terimin D_i ve Q belgelerindeki ağırlık değerlerinin çarpımlarının toplamı ile hesaplanır.

$D_1 \bullet Q = 0.00619$,

$D_2 \bullet Q = 0.00108$ olarak elde edilir.

Bu hesaplamaların ardından, D_1 ve Q ile D_2 ve Q vektörleri arasındaki açıların kosinüs değerleri;

$\cos(D_1,Q) = 0.803$,

$\cos(D_2,Q) = 0.203$ olarak elde edilir.

Burada $\cos(D_1,Q) > \cos(D_2,Q)$ olduğu için, Q sorgu verisi D_1 eğitim verisi sınıfına daha benzerdir denilebilir. Benzerlik oranları Eş. 4.4 ve Eş. 4.5 ile hesaplanır.

$$\text{Benzerlik}(D_1,Q) = 100 * P(D_1,Q) / [P(D_1,Q) + P(D_2,Q)] \quad (4.4)$$

Eş. 4.4'ye göre, $\text{Benzerlik}(D_1,Q) = \%79.8$,

$$\text{Benzerlik}(D_2,Q) = 100 * P(D_2,Q) / [P(D_1,Q) + P(D_2,Q)] \quad (4.5)$$

Eş. 4.5'e göre, $\text{Benzerlik}(D_2,Q) = \%20.2$ olarak elde edilir.

Eş. 4.4 ve Eş. 4.5'teki hesaplamalar sonucunda, Q sorgu kümesinin D_1 sınıfına benzerlik oranı %79,8, D_2 sınıfına benzerlik oranı %20.2 olduğu görülmektedir. D_1 sınıfına daha yakın olan Q sorgu verisinin spam olduğu sonucuna varılmaktadır.

4.3.6. Tweet içeriğindeki kötücül linklerin tespit edilmesi

Tweet içeriğinde spam içerikli metinlerin yanı sıra çeşitli spam ve ya kötücül içerik içerik barındıran web sayfalarına yönlendirme yapan linkler'de yer alabilmektedir.

Kötücül içeriklerin yer aldığı örnek bir kara listede yer alan bazı web sayfaları Çizelge 4.8'de görülmektedir.

Çizelge 4.8. Kötücül içeriklerin yer aldığı bazı web adresleri

Kötücül içeriklerin yer aldığı bazı linkler		
114oldest.com	de007.net	mamj.ru
18dd.net	deunce68rtaint.rr.nu	mampoks.ru
18xn.com	dionneg.com	maniyakat.cn
1a-teensbilder.de	dj-cruse.de	marcasdelnorte.com.mx
2000tours.com	doctorvj.com	mariposita.web-personal.org
318x.com	dongsungmold.com	martuz.cn
38zu.cn	douate.com	masterkey.com.ua
4safe.in	e-taekwang.com	matthewsusmel.com
888758.com	eloyed.com	matzines.com
abcmlm.com	eplarine.com	mefa.ws
acd.com.vn	etnkorea.com	microsearchstat.com
acusticjjw.pl	fancycake.net	microsotf.cn
admagnet1.com	fashion-ol.com.pl	mjw.or.kr
advabnr.com	ff.fjpark.com	mnogobab.com
ali59000.free.fr	filmschoolsforum.com	mobile-content.info
alphaxiom.com	firoznadiadwala.com	mogyang.net
altan5.com	fishum.com	monidopo.bee.pl
amusecity.com	fnyoga.biz	motionritm.ru
an4u.com	gabriellerosephotography.com	mst.com.ua
anayaoeventos.com	gamegoldonline.in	mulbora.com
ap-transz.hu	gassystem.co.kr	mygooglemy.com
appprices.com	gavih.org	n85853.cn
armazones.com	gclabrelscon.net	narbhaveecareers.com
arta.romail3arnest.info	ghura.pl	natebennettfleming.com

Çizelge 4.8'de görülen ve kötücül içerikler ihtiva eden web siteleri tweet içeriklerinde sıklıkla yer alabilmektedir.

Kısa link'lerin normal hale dönüştürülmesi

Çoğu tweet içeriğindeki linkler kısa link halindedir. Bu linklerin kötücül olup olmadığının tespiti için ilgili linklerin normal hallerine dönüştürülmesi gerekmektedir. Bazı link kısaltma siteleri ve örnek kısa linkler Çizelge 4.9'da görülmektedir.

Çizelge 4.9. Bazı link kısaltma siteleri ve oluşturdukları örnek kısa linkler

Link Kısaltma Sitesi	**Örnek Kısa Link**
adf.ly	http://adf.ly/1KXfby
bit.ly	http://bit.ly/1Cu0ll1
goo.gl	http://goo.gl/W0Csaa
tinyurl	http://tinyurl.com/oh9vttm
bc.vc	http://bc.vc/1y4bRH
ow.ly	http://ow.ly/PqLdZ
adfoc.us	http://adfoc.us/x55863324
tiny.cc	http://tiny.cc/onlf0x
ıs.gd	http://is.gd/mf34rR
bit.do	http://bit.do/63FL
tr.im	https://tr.im/CYj8I
mcaf.ee	http://mcaf.ee/fjx6t
u.to	http://u.to/3_j0Cw
gg.gg	http://gg.gg/3sctt

Çizelge 4.9'daki kısa linklerin normal hale getirilmesi için Java'nın sunduğu "java.net.URL" kütüphanesinden yararlanılmıştır. Şekil 4.25'teki kod bloğu yardımı ile kısa linklerin normal hale çevrilmesi sağlanabilmektedir.

```
public static String expandUrl(String shortenedUrl) {
URL url = new URL(shortenedUrl);
HttpURLConnection httpURLConnection
=(HttpURLConnection) url.openConnection(Proxy.NO_PROXY);
httpURLConnection.setInstanceFollowRedirects(false);
String expandedURL
=httpURLConnection.getHeaderField("Location");
httpURLConnection.disconnect();
return expandedURL;
```

Şekil 4.25. Kısa linklerin normal (uzun) hale çevriren kod bloğu

Şekil 4.25'teki Java kod bloğu yardımıyla bir kısa link oluşturma websitesi yardımıyla oluşturulan kısa linkler normal hallerine dönüştürülebilmektedir.

Tweet içeriklerinde yer alan linklerin kötücül olup olmadığının tespiti için bazı güvenlik araçları kullanılabilmektedir. Bunların bazıları aşağıdaki tabloda gösterilmektedir.

Çizelge 4.10. Bazı güvenlik araçları ve web adresleri

Güvenlik Aracı	**Web Adresi**
Google safebrowsing API	www.google.com/safebrowsing
VirusTotal	www.virustotal.com
URL Void	www.urlvoid.com
Metascan Online	https://www.metascan-online.com
Exposure	http://exposure.iseclab.org/
Malware Domain List	http://www.malwaredomainlist.com/mdl.php
Malc0de Database	http://malc0de.com/database/
PhishTank	www.phishtank.com
SURBL Blaclist Lookup	http://www.surbl.org/surbl-analysis
URLVir	http://www.urlvir.com/
FortiGuard	http://www.fortiguard.com/ip_rep/index.php
Norton Safe Web	https://safeweb.norton.com
AVG ThreatLabs	avgthreatlabs.com/sitereports
SpamHaus Domain Block List	http://www.spamhaus.org/lookup/
ThreatLog	http://www.threatlog.com/
urlQuery	http://urlquery.net
Webutation	www.webutation.net
Sucuri SiteCheck	sitecheck.sucuri.net/scanner

Çizelge 4.10'da yer alan güvenlik araçları genellikle kötücül içerikli sitelerin yer aldığı bir kara liste oluşturup ilgili web sayfasının bu kara listede olup olmadığının kontrolü mantığı ile çalışmaktadır.

Uygulamada kötücül içeriklere sahip olan linklerin tespiti için kullanılan güvenlik araçlarından Google SafeBrowsing API'si kullanılmıştır. Bunun için öncelikle kullanılan googlesafebrowsing API'sine ait oluşturulan uygulama adı, uygulama anahtar değeri, uygulama versiyonu, program versiyonu değerleri Şekil 4.26'daki Java kod bloğu ile gerçekleştirilebilmektedir.

```
String googlesafebrowsing= "";
googlesafebrowsing+=URLEncoder.encode("client")+"
="+URLEncoder.encode("myapp", "UTF-8") + "&";
googlesafebrowsing+=URLEncoder.encode("apikey")+"
="+URLEncoder.encode("APIKEY", "UTF-8")+"&";
googlesafebrowsing+=URLEncoder.encode("appver")+"
="+URLEncoder.encode("1.5.2", "UTF-8") + "&";
googlesafebrowsing+=URLEncoder.encode("pver","UTF-8")+"
="+ URLEncoder.encode("3.0", "UTF-8");
```

Şekil 4.26. Googlesafebrowsing API'sinin kullanılması için oluşturulan kod bloğu

Şekil 4.26'da görüldüğü gibi googlesafebrowsing API'si için gerekli uygulama adı ve anahtar değerler ilgili kod bloğu ile girilebilmektedir. Daha sonra ilgili API sayesinde girilen web adresinin kötücül olup olmadığı belirlenir. İlgili işlem Şekil 4.27'deki kod bloğunda görülmektedir.

```
String baseURL = "https://sb-ssl.google.com/safebrowsing/api/lookup?client=demo-app
&apikey=ABQIAAAAJIThQVNDY5dSzWw6_ovAoZkwQ&appver=1.5.2&pver=3.0&url=";
String subjectURL = "KONTROL_EDILECEK_ADRES";
output = getHttpResponseRabby(baseURL+subjectURL);
```

Şekil 4.27. Bir web sitesinin kötücül olup olmadığını belirleyen kod bloğu

Şekil 4.27'deki kod bloğu yardımıyla ilgili adresin kötücül olup olmadığı tespit edilmektedir. Bazı durumlarda ise tweet içeriğindeki link normal içeriğe sahipken, ilgili link yardımıyla yönlendirme yapılan web içeriğinde kötücül içerikli linkler olmaktadır. Bu nedenle ilgili linke ait web sayfasının içeriğinin taranıp, içeriğinde yer alan linklerin de taranması gerekebilmektedir. Bu işlemler için uygulamada, Java'nın sunduğu "org.jsoup.Jsoup" kütüphanesinden yararlanılmıştır. Bir web sayfası içeriğinde yer alan linklerin listesi Şekil 4.28'de yer alan kod bloğu yardımıyla elde edilebilmektedir.

```
String url = WEB_ADRESİ;
print(url);
Document doc = Jsoup.connect(url).get();
Elements links = doc.select("a[href]");
Elements media = doc.select("[src]");
Elements imports = doc.select("link[href]");

print("\nLinks: (%d)", links.size());
for (Element link : links) {
print("%s", link.attr("abs:href"));
```

Şekil 4.28. Girilen bir web sitesinin içeriğinde yer alan linkleri tespit eden kod bloğu

Şekil 4.28'de yer alan Java kod bloğu sayesinde girilen bir web sitesinin içeriği taranarak, ilgili web sitesinin içeriğinde mevcut olan bir linklerin tespit edilmesi sağlanmaktadır.

4.4. Deneysel Çalışmaya İlişkin Başarım Oranları

Deneysel çalışmaya ilişkin başarım sonuçlarının bulunmasında çeşitli değerlendirme ölçütleri kullanılmıştır. Bunlar Geri Çağırma (Recall), Doğruluk (Accuracy), Duyarlılık (Precision), Seçicilik (Selectivity) ve F-Ölçütü (F-Score) ölçütleridir. Gerçi Çağırma; tüm spam sınıflardan ne kadarının doğru olarak tahmin edildiğidir. Doğruluk; doğru olarak yapılan tüm tahmin verilerinin, tüm sınıflarda yer alan verilere oranıdır. Duyarlılık; pozitif veriler içerisinden ne kadarının doğru olarak tahmin edildiğidir. Seçicilik; negatif veriler içerisinden ne kadarının doğru olarak tahmin edildiğidir. F-Ölçütü; Geri Çağırma ve Duyarlılık'ı aynı anda ölçmeye yardımcı olur. Bu ölçme tekniğinde aritmetik ortalama yerine harmonik ortalama kullanılmaktadır.

4.4.1. Türkçe içerikli tweet'ler için geliştirilen uygulama

Çalışmada gerçekleştirilen Türkçe uygulamada, Vektör Uzay Modeli'nde eğitim amaçlı yararlanılmak üzere, Uysal vd. tarafından oluşturulmuş 420 adet spam ve 430 adet spam olmayan Türkçe iletiler içeren TurkishSMS isimli veriseti kullanılmaktadır. Geliştirilen sistemin başarımının test edilmesi aşamasında, sorgu veriseti olarak kullanılmak üzere çeşitli internet sitelerinden elde edilen ve el yordamı ile sınıflandırılan, 200 adet spam ve 200 adet spam olmayan olmak üzere, Twitter iletisi niteliğinde Türkçe yazılmış ifadeler içeren TurkishSpamTwitter isimli veriseti oluşturulmuştur [46].

Çizelge 4.11. Türkçe verisetine ilişkin içerik bilgileri

	Eğitim Veri Seti	**Sorgu Veri Seti**
Spam Mesaj Sayısı	420	200
Spam Olmayan Mesaj	430	200
Toplam Mesaj Sayısı	850	400
Genel Toplam Mesaj Sayısı	1250	

Çizelge 4.11'de görüldüğü gibi çalışmada Vektör Uzay Modeli'nde kullanılmak üzere toplamda 1250 iletiden oluşan eğitim ve sorgu veri seti kullanılmaktadır. Yapılan çalışmaya ait karmaşıklık matrisi Çizelge 4.12'de görülmektedir.

Çizelge 4.12. Karmaşıklık matrisi

		Gerçek	
Tahmin	Spam Mesaj	Doğru Pozitif (a)	Yanlış Negatif (b)
	Spam Olmayan Mesaj	Yanlış Pozitif (c)	Doğru Negatif (d)

Çizelge 4.12'deki karmaşıklık matrisinde yer alan veriler yardımıyla çalışmanın başarım oranlarının belirlenmesi için kullanılan değerlendirme ölçütlerine (Geri Çağırma, Doğruluk, Duyarlılık, Seçicilik, Yanlış Pozitif Oranı, Yanlış Negatif Oranı, F-Ölçütü) ilişkin hesaplamalar Eş. 4.6 - 4.12'de görülmektedir.

Geri Çağırma (Recall) = a/(a+b) (4.6)

Doğruluk (Accuracy)= (a+d)/ (a+b+c+d) (4.7)

Duyarlılık (Precision) (Doğru Pozitif Oranı) = a/(a+c) (4.8)

Seçicilik (Doğru Negatif Oranı) (Selectivity) = d/(b+d) (4.9)

F-Ölçütü (F-Score) = 2a/(2a+b+c) (4.10)

Yanlış Pozitif Oranı = b/(b+d) (4.11)

Yanlış Negatif Oranı = c/ (c+a) (4.12)

Eş. 4.6-4.12'deki hesaplamalara ilişkin elde edilen sonuçlar Çizelge 4.13 ve Çizelge 4.14'te görülmektedir.

Çizelge 4.13. Performans başarım oranları

Değerlendirme Ölçütü	**Çalışmanın Başarım Oranı**
Geri Çağırma	188/(188+12) =0.94
Doğruluk	(188+194)/(188+12+6+194) = 0.97
Duyarlılık (Doğru Pozitif)	188/(188+6) = 0.96
Seçicilik (Doğru Negatif)	194/(12+194) = 0.94
F-Ölçütü	(2*188)/(2*188+12+6) = 0.95

Çizelge 4.14 Performans hata oranları

Değerlendirme Ölçütü	Çalışmanın Hata Oranı
Yanlış Pozitif	12/(12+194) = 0.05
Yanlış Negatif	6/(6+188) = 0.03

Çizelge 4.13 ve Çizelge 4.14'te görüldüğü gibi yapılan çalışmanın başarım ve hata oranlarının belirlenmesinde ilgili değerlendirme ölçütleri kullanıldığında; Geri Çağırma Değeri: %94, Doğruluk Değeri: %97, Duyarlılık Değeri: %96, Seçicilik Değeri: %94, F-Ölçütü: %95, Yanlış Pozitif Değeri: %5 ve Yanlış Negatif Değeri: %3 olarak elde edilmektedir.

4.4.2. İngilizce içerikli tweet'ler için geliştirilen uygulama

Çalışmada İngilizce tweet'ler üzerinde yapılan analiz işlemlerinde [47] ve [48] 'de yer alan verisetleri birleştirilerek toplamda 7044 adet mesaj içeren bir Eğitim veriseti oluşturulmuştur. Ayrıca [49], [50] ve [51]'ten elde edilen mesaj içerikleri derlenerek toplamda 6225 adet mesaj içeren bir Sorgu veriseti elde edilmiştir. İlgili sorgu ve eğitim verisetlerinin içeriklerine ilişkin bilgiler Çizelge 4.15'te görülmektedir.

Çizelge 4.15. İngilizce verisetine ilişkin içerik bilgileri

	Eğitim Veri Seti	Sorgu Veri Seti
Spam Mesaj Sayısı	1211	1464
Spam Olmayan Mesaj	5833	4761
Toplam Mesaj Sayısı	7044	6225
Genel Toplam Mesaj Sayısı	13269	

Çizelge 4.15'te görüldüğü gibi çalışmada Vektör Uzay Modeli'nde kullanılmak üzere toplamda 13269 iletiden oluşan eğitim ve sorgu veri seti kullanılmaktadır. Yapılan çalışmaya ait karmaşıklık matrisi Çizelge 4.16'te görülmektedir.

Çizelge 4.16. Karmaşıklık matrisi

		Gerçek	
Tahmin	Spam Mesaj	Doğru Pozitif (a)	Yanlış Negatif (b)
	Spam Olmayan Mesaj	Yanlış Pozitif (c)	Doğru Negatif (d)

Çizelge 4.16'daki karmaşıklık matrisinde yer alan veriler yardımıyla çalışmanın başarım oranlarının belirlenmesi için kullanılan değerlendirme ölçütlerine (Geri Çağırma, Doğruluk,

Duyarlılık, Seçicilik, Yanlış Pozitif Oranı, Yanlış Negatif Oranı, F-Ölçütü) ilişkin hesaplamalar Eş. 4.6-4.12'de görülmektedir.

Eş. 4.6-4.12'deki hesaplamalara ilişkin elde edilen sonuçlar Çizelge 4.17 ve Çizelge 4.18'de görülmektedir.

Çizelge 4.17. Performans başarım oranları

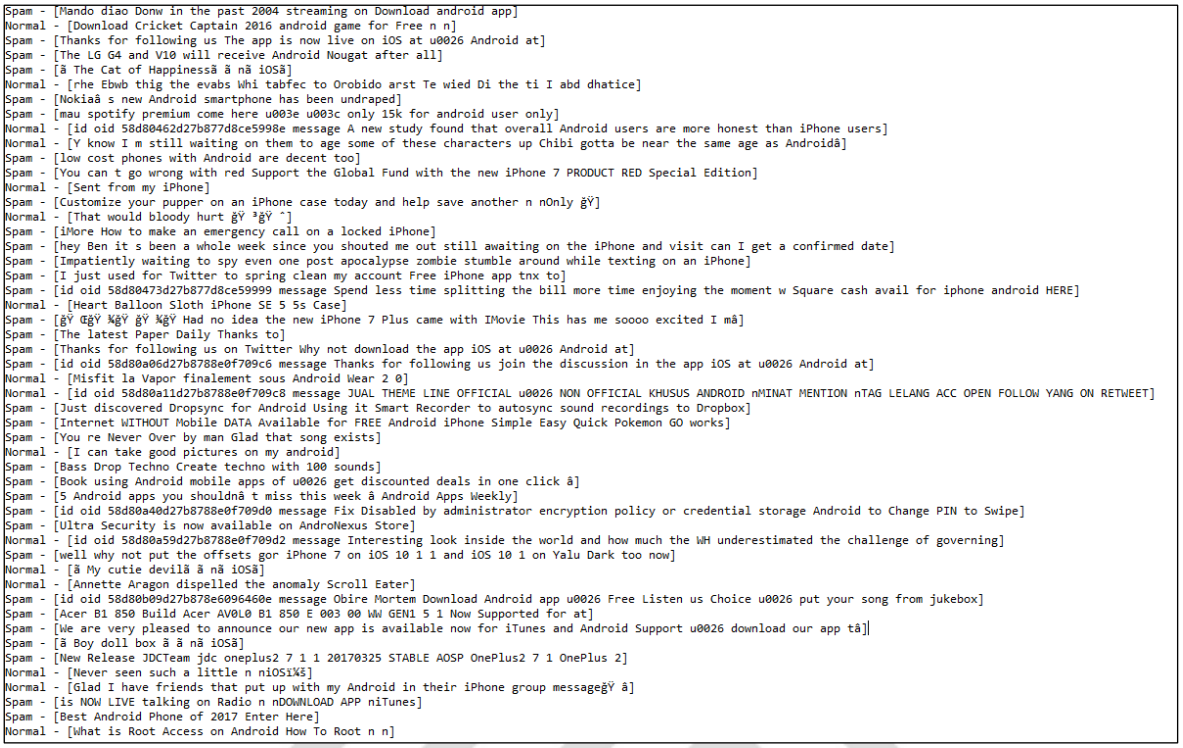
Değerlendirme Ölçütü	Çalışmanın Başarım Oranı
Geri Çağırma	1348/(1348+116) = 0.92
Doğruluk	(1348+4416)/(1348+116+345+4416) = 0.92
Duyarlılık (Doğru Pozitif)	1348/(1348+345) = 0.79
Seçicilik (Doğru Negatif)	4416/(116+4416) = 0.97
F-Ölçütü	(2*1348)/(2*1348+116+345) = 0.85

Çizelge 4.18 Performans hata oranları

Değerlendirme Ölçütü	Çalışmanın Hata Oranı
Yanlış Pozitif	116/(116+4416) = 0.02
Yanlış Negatif	345/(345+1348) = 0.20

Çizelge 4.17 ve Çizelge 4.18'de görüldüğü gibi yapılan çalışmanın başarım ve hata oranlarının belirlenmesinde ilgili değerlendirme ölçütleri kullanıldığında; Geri Çağırma Değeri: %92, Doğruluk Değeri: %92, Duyarlılık Değeri: %79, Seçicilik Değeri: %97, F-Ölçütü: %85, Yanlış Pozitif Değeri: %2 ve Yanlış Negatif Değeri: %20 olarak elde edilmektedir.

Yapılan çalışmanın başarım tespitinin haricinde ayrıca; Twitter üzerinden çeşitli etiketleri içeren (#iphone, #android, #followback, #linux, #windows, #android, #technology, #pokemongo) 24532 adet İngilizce içerikli tweet Java ile yazılmış bir program ile çekilerek MongoDB veritabanına kaydedilmiştir. Twitter'ın kullanıcı sayısının fazlalığı ve sürekli veri akışlı yapısı (tweet), veri ambarının yüksek hızlı veri depolayabilmesini gerektirmektedir. Bu ihtiyaçtan MongoDB veritabanı kullanılmıştır [52]. MongoDB ölçeklenebilir bir yapı sunan ve doküman tabanlı bir NoSQL bir veritabanıdır. Hızlı işlem yapılması gereken işlemlerde (büyük hacimli problemler, caching sistemler, web içerik yönetim sistemleri, sosyal medya yorum/etiket saklama) kullanılması büyük avantaj sağlamaktadır [53]. MongoDB veritabanındaki bu 24532 adet tweet üzerinde Vektör Uzay Modeli kullanılarak spam tespiti gerçekleştirilmiştir. Elde edilen sonuçlara ait bir kesit Şekil 4.29'da görülmektedir.

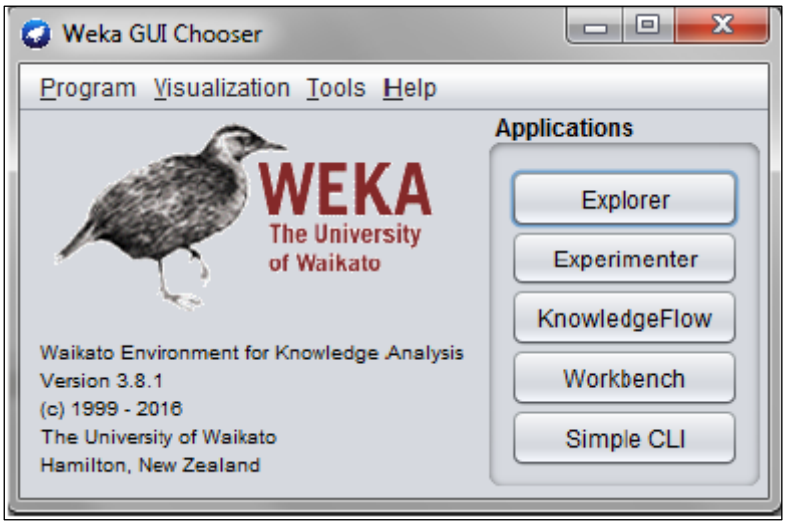


Şekil 4.29. Test verileri için gerçekleştirilen analiz sonuçlarına ait örnek bir kesit

Şekil 4.29'deki analiz sonuçlarına ilişkin kesitte görüldüğü Twitter'dan çekilip MongoDB veritabanında saklanan 24532 adet tweet Vektör Uzay Modeli yardımıyla analiz edilerek spam olup olmadığı belirlenmiştir.

4.4.3. WEKA ve yapılan çalışmanın WEKA ile karşılaştırılması

WEKA (Waikato Environment for Knowledge Analysis) Waikato Üniversitesinde bir proje olarak kullanılmakta iken giderek kullanımı yaygınlaşmış bir veri madenciliği uygulamasıdır. İçeriğinde birçok sınıflandırıcı algoritmalar yer alana açık kaynak kodlu ücretsiz bir yazılımdır [54]. Veri madenciliğinde kullanılmak üzere girilen veriler üzerinde öğrenme ve öğrendiklerinden yola çıkarak yeni veriler üzerinde sınıflandırma tahmini yapan bir uygulamadır. Desteklediği veriler, arff, csv, c45, libsvm, svmlight, xarff formatlarıdır. Jdbc sürücüsünü destekleyen veritabanlarına bağlantı yapabilme ve http protokolü yardımıyla uygun formatlardaki dosyaları kullanıp işleyebilme özelliği mevcuttur [55]. Şekil 4.30'da WEKA'nın giriş ekranı görülmektedir.



Şekil 4.30. WEKA'ya ait giriş ekran görüntüsü

Şekil 4.30'daki WEKA ana ekranında yer aldığı üzere WEKA'nın desteklediği veri madenciliğine ait işlemler Program menüsü altında görülebilmektedir. Bu işlemler Preprocess (Ön hazırlık), Classify (Sınıflandırma), Cluster (Kümeleme), Associate (Birliktelik), Select Attributes (Özellik seçimi) ve Vizualize (Görselleştirme) işlemleridir [56].

WEKA içeriğinde 71 adet algoritmayı barındırır. Bu algoritmalar işlevlerine göre 6 kategoride sınıflandırılmıştır. Bu kategoriler: Bayes (BayesNet, Naive Bayes, Multinomial gibi Bayes sınıflayıcılar Bayes sınıflayıcılar), Functions (Logistic, SimpleLogistic, LibLINEAR, LibSVM, RBFNetwork, SMO), Lazy (IB1, IBk, KStar), Meta (AdaBoostM1, Dagging, Bagging), Trees (J48, BFTree, ADTree) ve Rules(JRip, OneR, ZeroR) kategorileridir. WEKA'da veriler 'arff' formatında saklanır. 'arff' dosyası içerisindeki verilere ait öznitelikler virgülle ayrılarak gösterilmektedir. Daha sonra bu veriler bir metin dosyasına veya kullanılmak üzere bir programa yüklenerek kullanılabilmektedir. Dosya içerisinde @relation ile ilişkileri, @attribute ile öznitelik bilgilerini, @data ile ham metin belgesi olarak kaydedilmektedir. Örnek bir arff dosyası Şekil 4.31'de görülmektedir.

```
DATA SET:

DATA SET:
@relation 'data set'

@attribute text string
@attribute class {'no spam',spam,'?'}

@data
'hey, buy this from me!',spam
'do you want to buy?',spam
'I have a party tonight!','no spam'
'today it is a nice weather','no spam'
'you are best',spam
'I have a horse','no spam'
'you are my friend','no spam'
'buy, buy, buy!',spam
'it is spring in the air','no spam'
'do you want to come?','no spam'
```

Şekil 4.31. Örnek bir arff dosyası

Şekil 4.31'deki arff dosyasında görüleceği üzere WEKA'nın üzerinde işlem yapacağı verilere ait nitelikler ve bu niteliklere ait içerik bilgileri sisteme giriş olarak verilmektedir. WEKA ile yapılan spam/spam olmayan mesaj sınıflandırma çalışmasında Weka-3.7.0 kütüphanesi kullanılarak WEKA'ya ait algoritmalara erişim sağlanabilmektedir. İlgili kütüphane kullanılarak erişilebilen bazı WEKA algoritmaları Şekil 4.32'de görülmektedir.

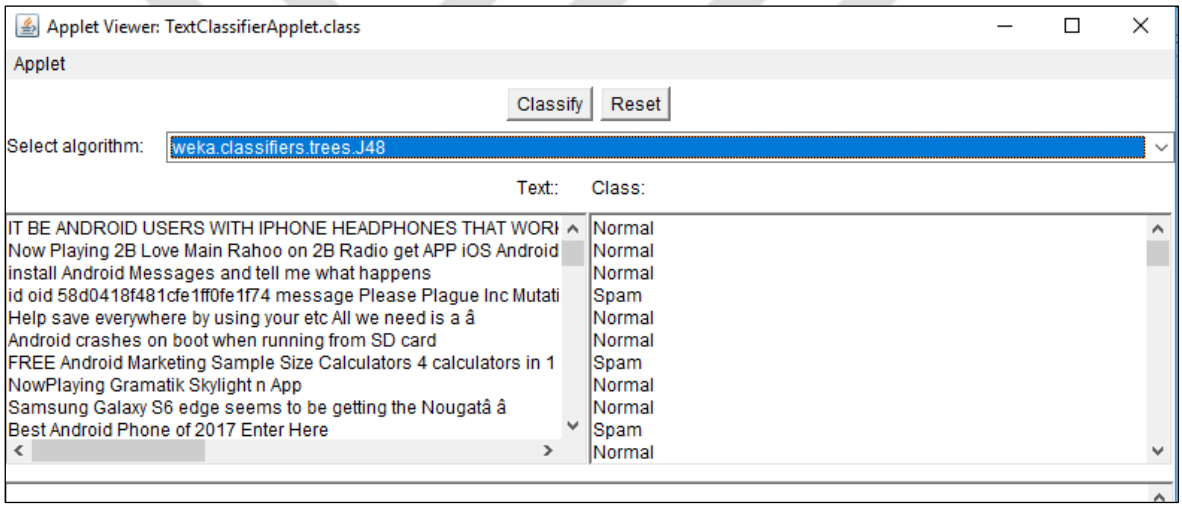
```
algorithmChoice.addItem("weka.classifiers.lazy.IB1");
algorithmChoice.addItem("weka.classifiers.lazy.IBk");
algorithmChoice.addItem("weka.classifiers.functions.SMO");
algorithmChoice.addItem("weka.classifiers.functions.MultilayerPerceptron");
algorithmChoice.addItem("weka.classifiers.functions.Logistic");
algorithmChoice.addItem("weka.classifiers.lazy.KStar");
algorithmChoice.addItem("weka.classifiers.misc.HyperPipes");
algorithmChoice.addItem("weka.classifiers.misc.VFI");
algorithmChoice.addItem("weka.classifiers.rules.PART");
algorithmChoice.addItem("weka.classifiers.rules.ConjunctiveRule");
algorithmChoice.addItem("weka.classifiers.rules.DecisionTable");
algorithmChoice.addItem("weka.classifiers.rules.JRip");
algorithmChoice.addItem("weka.classifiers.rules.NNge");
algorithmChoice.addItem("weka.classifiers.rules.Ridor");
algorithmChoice.addItem("weka.classifiers.rules.OneR");
algorithmChoice.addItem("weka.classifiers.trees.J48");
algorithmChoice.addItem("weka.classifiers.trees.REPTree");
```

Şekil 4.32. WEKA'nın içeriğindeki bazı algoritmalar

Şekil 4.32'de görüldüğü gibi Weka-3.7.0 kütüphanesi yardımıyla çeşitli WEKA algoritmalarına erişim sağlanıp, bu algoritmalar spam içerik tespitinde kullanılabilmektedir. WEKA ile yapılan spam tespiti çalışmasında WEKA'nın içeriğinde yer alan algoritmalardan

- "weka.classifiers.bayes.NaiveBayes";
- “weka.classifiers.functions.SMO";
- "weka.classifiers.lazy.IB1";
- "weka.classifiers.trees.RandomForest";
- "weka.classifiers.trees.J48";
- "weka.classifiers.functions.Logistic" algoritmaları kullanılmıştır.

WEKA’ya çalışmada kullanılan İngilizce içerikli eğitim verisetindeki 7044 adet ileti eğitim amaçlı olarak tanımlanmış ve sonrasında sorgu verisetinde yer alan 6225 adet ileti ile sistemin yukarıda belirtilen altı adet algoritma ile test edilmiştir. İletiler üzerinde herhangi bir ön işlem yapılmadan sisteme girişleri yapılmıştır. Weka 3.7.0 kütüphanesi kullanılarak yapılan çalışmaya ilişkin ekran görüntüsü Şekil 4.33‘te görülmektedir.



Şekil 4.33. Weka 3.7.0 kullanılarak geliştirilen uygulamaya ilişkin örnek bir kesit

Çalışmada Vektör Uzay Modeli kullanılarak elde edilen başarım ile WEKA içerisinden seçilen algoritmalara ilişkin elde edilen başarım oranları Çizelge 4.19‘da görülmektedir.

Çizelge 4.19 WEKA kullanılarak gerçekleştirilen çalışmaya ait başarım oranları

Algoritma/Metot	**Başarım Oranı**
weka.classifiers.bayes.NaiveBayes	%93
weka.classifiers.functions.SMO	%90
weka.classifiers.lazy.IB1	%87
weka.classifiers.trees.RandomForest	%94
weka.classifiers.trees.J48	%91
weka.classifiers.functions.Logistic	%89
Vektör Uzay Modeli	%92

Çizelge 4.19’da görüldüğü gibi WEKA’da yer alan ilgili makine öğrenmesi yöntemleri ile karşılaştırıldığında Vektör Uzay Modeli’nin de makine öğrenmesi yöntemleri gibi başarılı sonuçlar verdiği görülmektedir. Bu yöntemler arasından Random Forest ve Naive Bayes metotlarının diğerlerinden daha başarılı sonuçlar verdiği görülmektedir.

5. SONUÇ

Spam tweet'ler Twitter'da gereksiz trafik oluşturarak kaynak ve zaman israfına neden olan iletilerdir. Spam tweet'ler genellikle firmalardan gelen reklam amaçlı mesajlar, bahis veya pornografik içerikli yasadışı internet sayfalarına yönlendirme yapan iletiler ile propaganda amaçlı gönderilmiş içeriklerden oluşmaktadır.

Çalışmada Twitter içeriklerinde yer alan istenmeyen iletilerin tespiti gerçekleştirilmiştir. Bunun için istenilen bir etiketi içeren (hastag) Türkçe veya İngilizce içeriklere sahip tweet'ler Java dilinde yazılmış bir uygulama ile Twitter'ın kullanıcılara sunduğu API vasıtası ile çekilmiştir. Çekilen tweet'ler MongoDB veritabanı yardımıyla kaydedilmiştir. Ardından ön-işlem aşamalarından geçirilen tweetlerin Vektör Uzay Modeli yardımıyla spam olup olmadığı belirlenmiştir.

Çalışmanın başarısının tespiti için literatürde yer alan ve spam olup olmadığı etiketlenmiş iletiler içeren verisetlerinden yararlanılmıştır. Bu verisetlerinde yer alan verilerin bir kısmı eğitim kalan kısmı ise sorgu veriseti olarak belirlenmiştir. Ön işlem aşamalarından geçirilen verisetlerindeki veriler Vektör Uzay Modeli ile eğitim ve sorgu aşamalarından geçirilmiştir. Yapılan deneysel çalışmalar neticesinde İngilizce tweet'ler üzerinde yapılan spam ileti tespiti analizinde %92, Türkçe tweet'ler üzerinde yapılan spam tespiti analizinde ise %97 oranında bir başarım ile sınıflandırma işlemi gerçekleştirilmiştir.

Çalışmada Vektör Uzay Modeli'nin yanısıra WEKA kullanılarak Naive Bayes, SMO, IB1, Random Forest, Logistic ve J48 yöntemleri de ilgili probleme uygulanmıştır. Bu yöntemlerin arasından en başarılı olanların Naive Bayes (%93) ve Random Forest (%94) yöntemleri olduğu görülmüştür.

Literatürdeki yapılan çalışmalar incelendiğinde spam tespiti çalışmalarının genellikle İngilizce içerikli iletiler üzerinde yapıldığı görülmektedir. Türkçe içerikli iletiler için yapılan çalışmalar sınırlıdır. Literatürde bu alanda Türkçe içerikli verisetlerinin yok denilecek kadar az olduğu görülmektedir. Yapılan bu çalışmanın Tükçe içerikli iletiler için de yapılmış olması bu açıdan önemlidir.

Gelecekte, Türkçe ve İngilizce içerikli iletiler üzerinde spam tespiti işleminde birden fazla makine öğrenmesi yönteminin birlikte uygulandığı hibrit sistemler geliştirilmesi amaçlanmaktadır.

KAYNAKLAR

1. İnternet: Global Digital Statshot report. URL: https://wearesocial.com/blog/2019/07/global-social-media-users-pass-3-5-billion, Son Erişim Tarihi: 06.09.2019.

2. İkizler, M., Başar, S. (2006). Spam'in Zararları ve Spam ile Hukuki Mücadele: ABD Örneği ve Türk ve Avrupa Birliği Hukukları ile Karşılaştırılması. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* 8(2), 91-114.

3. Liew, S.W., Sani, N.F.M., Abdullah M.T., Yaakob, R. (2018). Improvement of classification features to increase phishing tweets detection accuracy. *Journal of Theoretical and Applied Information Technology*. 96(10), 2900-2910.

4. Gunawan, D., Rahmat, R.F., Putra, A., Pasha, M.F. (2018, November). Filtering Spam Text Messages by Using Twitter-LDA Algorithm. *2018 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*. Medan, Indonesia.

5. Nauta, M. (2016, July). Detecting Hacked Twitter Accounts by Examining Behavioural Change using Twitter Metadata. *25th Twente Student Conference on IT*. Porto, Portugal.

6. Perveen, N., Missen, M.M.S., Rasool, Q., Akhtar, N. (2016). Sentiment Based Twitter Spam Detection. *International Journal of Advanced Computer Science and Applications(IJACSA)* 7(7), 568-573.

7. Cao, C., Caverlee, J. (2015, March). Detecting Spam URLs in Social Media via Behavioral Analysis. *European Conference on Information Retrieval Advances in Information Retrieval.* 703-714. Vienna, Austria.

8. Wang, B., Zubiaga, A., Liakata, M., Procter, R.N. (2015, May). Making the Most of Tweet-Inherent Features for Social Spam Detection on Twitter. *WWW Workshop on Making Sense of Microposts.* Florence, Italy.

9. Hu, X., Tang J., Liu, H. (2014, July). Online social spammer detection. *28th AAAI Conference on Artificial Intelligence,* 59-65. Québec, Canada.

10. Martinez-Romo, Araujo, J.L. (2013). Detecting malicious tweets in trending topics using a statistical analysis of language. *Expert Systems with Applications*, 40(8), 2992-3000.

11. Sangho, L., Jong, K. (2012, February). WarningBird: Detecting Suspicious URLs in Twitter Stream. *In NDSS*, (12) 1–13.

12. Song, J., Sangho, L., Jong, K. (2011, September). Spam Filtering in Twitter Using Sender-Receiver Relationship. *Recent Advances in Intrusion Detection: 14th International Symposium.* 301-307. CA, USA.

13. McCord, M., Chuah M. (2011, September). Spam detection on twitter using traditional classifiers. *ATC'11 Proceedings of the 8th international conference on Autonomic and trusted computing,* 175-186. Alberta, Canada.

14. Benevenuto, F., Magno, G., Rodrigues, T., Almeida, V. (2010, July). Detecting Spammers on Twitter. *Seventh annual Collaboration, Electronic messaging, AntiAbuse and Spam Conference (CEAS).* Washington, USA.

15. Kyumin, L., Caverlee, J., Webb, S. (2010, July). Uncovering social spammers: social honeypots + machine learning. *Proceedings of the 33rd international conference on Research and development in information retrieval,* 435-442. Geneva, Switzerland.

16. Sethi, G., Bhootna, V. (2014). SMS spam filtering application using Android. *Int. J. Comput. Sci. Inf. Technol.* 5(3), 4624-4626.

17. Ezpeleta, E., Zurutuza, U., Hidalgo, J.M.G. (2016, September). Short Messages Spam Filtering Using Sentiment Analysis. *International Conference on Text, Speech, and Dialogue.* Brno, Czech Republic.

18. Yang, Y., Hu, R., Qiu, C., Sun G., Li, H. (2017, June). A Spam Message Detection Model Based on Bayesian Classification. *International Conference on Emerging Internetworking, Data & Web Technologies.* Wuhan, China.

19. Bozan, Y.S., Çoban, Ö., Özyer G.T., Özyer, B. (2015, Mayıs). Metin Sınıflandırma ve Uzman Sistem Tabanlı İstenmeyen Kısa Mesajların Filtrelenmesi. *23nd Signal Processing and Communications Applications Conference (SIU).* Malatya, Turkey.

20. Akbari, F., Parast G.Z., Sajedi, H. (2015, May). SMS spam detection using selected text features and boosting classifiers. *Information and Knowledge Technology (IKT), 7th Conference on IEEE.* Urmiye, Iran.

21. Li, W., Zeng, S. (2016, August). A Vector Space Model based spam SMS filter. *Computer Science & Education (ICCSE),* Nagoya, Japan.

22. Wang, H.A. (2010, July). Don't follow me: Spam detection in Twitter. *International Conference on Security and Cryptography.* Athens, Greece.

23. Karasoy, O., Ballı, S. (2016, Haziran) İçerik Tabanlı İstenmeyen SMS Filtreleme için Mobil Uygulama Geliştirilmesi ve Sınıflandırma Algoritmalarının Karşılaştırılması. *International Artificial Intelligence and Data Processing Symposium.* Malatya, Turkey.

24. Özdemir, C., Ataş, M., Özer, A.B. (2013, April) Classification of Turkish spam e-mails with artificial immune system. *21st Signal Processing and Communications Applications Conference (SIU),* Haspolat, Turkey.

25. Çalış, K., Gazdağı, O., Yıldız, O. (2013) Reklam İçerikli Epostaların Metin Madenciliği Yöntemleri İle Otomatik Tespiti. *Bilişim Teknolojileri Dergisi.* 6(1), 1-7.

26. Barış, Ö. (2019). Geleneksel ve Sosyal Medya Gündem Uyumu İncelemesi: Twitter, Fox TV ve ATV Ana Haber Bülten Karşılaştırılması. *Erciyes İletişim Dergisi.* 6(1), 169-184.

27. İnternet: 2019 Türkiye İnternet Kullanım ve Sosyal Medya İstatistikleri. URL: https://dijilopedi.com/2019-turkiye-internet-kullanim-ve-sosyal-medya-istatistikleri/, Son Erişim Tarihi: 06.09.2019.

28. İnternet: Global Digital Report 2019. URL: - https://wearesocial.com/global-digital-report-2019, Son Erişim Tarihi: 06.09.2019.

29. Greenhow, C. (2009). Tapping the Wealth of Social Networks for Professional Development. *Learning & Leading with Technology*. 36(8), 10-11.

30. Güler, Ş. (2017). Twitter Hashtaglarinin Oluşturulma Sürecinin Nitel Bir Çalışma ile İncelenmesi: 2017 Anayasa Referandumu Örneği. *Uluslararası Sosyal Araştırmalar Dergisi*. 10(51), 985-993.

31. Salur, M.U., Aydın, İ. (2017). Üniversitelerin Paylaştığı Twitter Mesajlarının İnsanlara Erişiminin Bulanık Birliktelik Kuralları ile Değerlendirilmesi. *Harran Üniversitesi Mühendislik Dergisi.* 2(3), 25-39.

32. İnternet: Caroline Tag Veriseti. URL: http://etheses.bham.ac.uk/253/1/Tagg09PhD.pdf, Son Erişim Tarihi: 06.09.2019.

33. İnternet: TurkishSMS veriseti. URL: http://ceng.anadolu.edu.tr/par/, Son Erişim Tarihi: 06.09.2019.

34. İnternet: National University of Singapore (NUS) Corpus. URL: https://www.comp.nus.edu.sg/~rpnlpir/downloads/corpora/smsCorpus/, Son Erişim Tarihi: 06.09.2019.

35. İnternet: DIT SMS Spam Dataset. URL: http://www.dit.ie/computing/research/resources/smsdata/, Son Erişim Tarihi: 06.09.2019.

36. İnternet: Malay SMS corpus. URL: http://eprints.uthm.edu.my/6494/1/Cik_Feresa_Mohd_Foozy_U.pdf/, Son Erişim Tarihi: 06.09.2019.

37. İnternet: SMS Spam Corpus Collection. URL: http://www.esp.uem.es/jmgomez/smsspamcorpus/, Son Erişim Tarihi: 06.09.2019.

38. İnternet: UCI SMS Spam. URL: https://archive.ics.uci.edu/ml/datasets/SMS+Spam+Collection, Son Erişim Tarihi: 06.09.2019.

39. İnternet: Deceptive Opinion Spam Corpus v1.4. URL: http://myleott.com/op_spam/, Son Erişim Tarihi: 06.09.2019.

40. Bilgin, B. (2018). Makine Öğrenmesi Teori ve Algoritmaları, PapatyaBilim yayınları, 17-20.

41. Akın, A.A., Akın, M.D. (2007). An Open Source Natural Language Processing Library for Turkic Languages: Zemberek. *Electrical Engineering.* 431(38).

42. İnternet: Turkish Deasciifier. URL: https://ahmet.im/blog/turkish-deasciifier-for-java/, Son Erişim Tarihi: 06.09.2019.

43. Ulus, C. T., Ceyhan, E.B., Sağıroğlu Ş. (2015, Ekim). Bilgi Hasatlaması Yöntemleri ve Kişisel Bilgi Hasatlaması. *8.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*.

44. Salton, G., Allan J., Singhal, A. (1996). Automatic Text Decomposition and Structuring. Information Processing & Management, 32(2) 127-138.

45. Karamollaoğlu, H., Dogru, I. A., Dörterler M. (2018, Ekim). Detection of Spam E-mails with Machine Learning Methods, *Akıllı Sistemlerde Yenilikler ve Uygulamaları Konferansı.* Adana, Turkey.

46. İnternet: TurkishSpamSMS veriseti. URL: http://mobseclab.gazi.edu.tr/datasets/TurkishSpamSMS/, Son Erişim Tarihi: 06.09.2019.

47. İnternet: Kaggle_SMS_SPAM_HAM veriseti. URL: https://github.com/royanshul/Kaggle_SMS_SPAM_HAM/blob/master/spam.csv/, Son Erişim Tarihi: 06.09.2019.

48. İnternet: Sms-spam-ham-classification veriseti. URL: https://www.kaggle.com/annatu/sms-spam-ham-classification/data/, Son Erişim Tarihi: 06.09.2019.

49. İnternet: smsData veriseti. URL: http://docs.h2o.ai/h2o-tutorials/latest-stable/tutorials/data/smsData.txt, Son Erişim Tarihi: 06.09.2019.

50. İnternet: SpamCollection veriseti. URL: http://www.cs.tau.ac.il/~arielhe/ml12-project/ml12-project-results/with_dit_dataset/learning_algo/SMSSpamCollection_with_dit_learning_algo.txt, Son Erişim Tarihi: 06.09.2019.

51. İnternet: SMS Spam or Ham Text veriseti. URL: https://rpubs.com/hoakevinquach/SMS-Spam-or-Ham-Text Son Erişim Tarihi: 06.09.2019.

52. Gyorödi, C., Gyorödi, R., Pecherle, G., Olah, A. (2015, June). A comparative study: MongoDB vs. MySQL. *13th International Conference on Engineering of Modern Electric Systems (EMES)*. Oradea, Romania.

53. Eken, S., Kaya, F., Sayar, A., Kavak, A. (2014, Mayıs). Doküman Tabanlı NoSQL Veritabanları: MongoDB ve CouchDB yatay ölçeklenebilirlik karşılaştırması. *7. Mühendislik ve Teknoloji Sempozyumu.* Ankara, Türkiye.

54. Dener, M., Dörterler, M., Orman, A. (2009, Şubat) Açık Kaynak Kodlu Veri Madenciliği Programları: WEKA'da Örnek Uygulama. *Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı.* Şanlıurfa, Türkiye.

55. Coşkun, C., Baykal, A. (2011, Şubat) Veri Madenciliğinde Sınıflandırma Algoritmalarının Bir Örnek Üzerinde Karşılaştırılması. - *XIII. Akademik Bilişim Konferansı,* 51-58. Malatya, Türkiye.

56. Aksu, G., Doğan, N. (2019). Veri Madenciliğinde Kullanılan Bir Analiz Programı: WEKA. *Eğitimde ve Psikolojide Ölçme ve Değerlendirme Dergisi.* 10(1), 80-95.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı

Uyruğu

Doğum tarihi ve yeri

Medeni hali

Telefon

E-mail

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek Lisans	Gazi Üniversitesi / Bilgisayar Bilimleri	Devam ediyor
Lisans	K.T.Ü / Bilgisayar Mühendisliği	2009
Lise	Samsun Atatütk Anadolu Lisesi	2004

İş Deneyimi

Yıl	Yer	Görev
2010-2011	Bilim, Sanayi ve Teknoloji Bakanlığı	Bilgisayar Mühendisi
2011- Halen	Elektrik Üretim A.Ş.	Bilgisayar Mühendisi

Yabancı Dil

İngilizce

Yayınlar

1. Karamollaoğlu, H., Doğru, İ.A., Dörterler, M. (2018). Detection of Spam E-mails with Machine Learning Methods. *Innovations in Intelligent Systems and Applications Conference (ASYU)*. Adana, Turkey.

2. Karamollaoğlu, H., Doğru, İ.A., Dörterler, M., Utku, A. (2018). Sentiment Analysis on Turkish Social Media Shares through Lexicon Based Approach. *3rd International Conference on Computer Science and Engineering*. Sarajevo, Bosnia and Herzegovina.

3. Karamollaoğlu, H., Doğru, İ.A., Dörterler, M., Alkan M. (2018). Naïve Bayes Classifier Based Spam Detection on Turkish SMS Messages. *10th International Conference on Information Security and Cryptology*. Ankara, Turkey.

Hobiler

Müzik, Yüzme, Gezi, Sinema



GAZİLİ OLMAK AYRICALIKTIR...