Sınıflandırma Tabanlı Zombi Bilgisayar Tespit Sistemi

Deniz Kılınç, Fatma Bozyiğit, Emin Borandağ, Fatih Yücalar, Hasan Akyol, Emre Berk Akırmak, Zafer Uzun

[1] Celal Bayar Üniversitesi, Yazılım Mühendisliği Bölümü, Manisa

denizkilinc@cbu.edu.tr, fatma.bozyigi@cbu.edu.tr, emin.borandag@cbu.edu.tr, fatih.yucalar@cbu.edu.tr, hasan.akyol@ogr.cbu.edu.tr, emre.akirmak@ogr.cbu.edu.tr, zafer.uzun@ogr.cbu.edu.tr

Özet: Son yıllarda teknolojide meydana gelen yenilikler ve gelişmeler internet ortamında geliştirilen uygulamaların sayısını hızla arttırmış ve bu duruma paralel olarak da internet üzerinde güvenlik konusu önem kazanmıştır. Günümüzde çevrimiçi birçok saldırı yöntemi bulunmakta ve bu saldırılar sistemlerin hizmet veremeyecek duruma düşmelerine sebep olmaktadır. Mevcut saldırı yöntemlerinden en kritik olanlardan DDoS (Distributed Denial of Service) saldırısı ile milyonlarca zombi bilgisayar, hedef alınan sistemin kaldırabileceği yükün çok üzerinde anlık istek göndererek, sistemi cevap veremez hale getirmektedir. Mevcut yöntemler bu konuda yeterli düzeyde güvenliği sağlayamamaktadır. Bu çalışma ile kullanıcıların kendi bilgisayarlarının DDoS saldırıları için zombi bilgisayar olup olmadığının kontrolünün sağlanması amaçlanmıştır. Bu amaç doğrultusunda üzerinde makine öğrenmesine dayalı sınıflandırma algoritmaları kullanarak zombi bilgisayar tespiti yapılmıştır. Çalışma sonucunda, gerçek bir kullanım ağından ve zombi veri üreten bir araçtan elde edilen çıktılar üzerinde test edilen sınıflandırma algoritmaları arasında en iyi sonucu 0.9358 doğruluk oranı ile Rasgele Orman algoritmasının verdiği gözlemlenmiştir.

Anahtar Sözcükler: Siber güvenlik, DDoS, zombi bilgisayar tespiti, sınıflandırma algoritmaları.

Am I Zombie? : Classification Based Detection System of Zombie Computer

Abstract: Due to the rapid developments in technology in recent years, the number of applications in internet has been increased concordantly. After all, security issues have emerged on the cyber world. Today there are many types of online attack methods which cause systems to disable. One of the most detrimental attacks is DDoS (Distributed Denial of Service) that disables and overloads the target systems by sending a lot of requests at the same time. This study is intended to provide users control whether or not their personal computers are zombie in DDoS attacks. For this purpose, machine learning based classification algorithms are utilized to detect and identify zombie computers. All classification algorithms are evaluated on a dataset which is obtained from a real network and an application producing zombie outputs. Random Forest with accuracy of 0.9358 gives the best result among the tested classification algorithms.

Keywords: Cyber security, DDoS, detecting of zombie computers, classification algorithms.

1. Giriş

Günümüzde internet kullanıcılarının istekleri ve gereksinimleri doğrultusunda birçok web sitesi bulunmaktadır. Bireyler; iletişimde kalabilmek(Facebook, Twitter, LinkedIn, Mail vb.), bilgiye hızlıca ulaşabilmek, eğlenceli vakit geçirebilmek (film ve oyun siteleri), kendilerini tanıtabilmek (Bloglar), firmalar ürünlerinin reklamlarını yapabilmek,

Devletler ise vatandaşlarının hizmetini kolaylaştırmak için (e-Devlet) web dünyasında hizmet vermektedir.

Web dünyasında hizmet verebilmenin en önemli şartı ise güvenliktir çünkü günümüzde birçok saldırı yöntemi bulunmakta olup, bu saldırılar çevrimiçi hizmetlerin engellenmesine ve bilgilerimizin çalınmasını sebep olabilmektedir. Bu saldırılardan en önemlisi ise DOS saldırılarından DDoS (Distributed Denial of Service) dur [1]. Bu saldırının en büyük ve önlem alınamaz gücü zombi olarak adlandırılan milyonlarca bilgisayarın farkında olmadan bu saldırının parçası olması ve saldırılan sistemin erişilebilirliğini ortadan kaldırmasıdır.

DDoS saldırılarında istekler çok farklı konumlardan, çok farklı şekillerde geldiği için önlem almak zorlaşmaktadır. Mevcut yöntemlerden en sık kullanılanı merkezi olarak hizmet veren sistemi korumaya odaklanmaktır. Ancak donanım ve network kaynaklarının her zaman sınırlı olmasından dolayı bu önlemler yetersiz kalmıştır. Örneğin merkezde 10 Gbps bir router'ınız varsa ve size 11 Gbps trafik yollanırsa, merkez tarafında ne kadar akıllı yazılımınız olduğunun bir önemi kalmayacaktır.

Bu saldırılara karşı kullanılan diğer yöntem ise zombi bilgisayar tarafında anti virüs yazılımı kurmak ve kişisel güvenlik duvarını maksimum düzeyde açmaktır. Fakat anti virüs yazılımlarının bir bilgisayarın zombi olup olmaması ile değil bilgisayarda zararlı bir yazılım olup olmadığı ile ilgilendiği için her zaman çözüm sağlayamamaktadır. Ancak şans eseri bir şekilde zararlı bir yazılım tespit ederlerse ve o yazılım da bilgisayarın zombi olmasına neden oluyorsa, o zaman işe yarayabilirler. Kişisel güvenlik duvarlarının asıl amacı ise, bilgisayar ve internet arasında filtreleme görevi görüp, dışarıdaki bilinmeyen bir trafiğin bilgisayara erişimini engellemektir. Bilgisayardan dışarıya giden verinin filtrelenmesi sadece port düzeyinde yapılabilmektedir. Bilgisayarlarda dışarıya açılan bu portların kapatılması bilgisayarın interneti kullanamaması anlamına gelmektedir [2].

DDoS saldırılarını tamamen çözmek için gerekli olan yöntem ise zombi grubuna dâhil edilen bilgisayarları tespit etmek ve bu şekilde saldırıların önüne geçmektir. Bu türde siber atakların önüne geçmek için hazırlanmış mevcut çalışmalar bulunmaktadır. Livadas ve diğerleri çalışmalarında siber atak saldırılarında sıklıkla kullanılan botnet grubuna dahil olan bilgisayarları belirlemeyi amaçlamış, bunun için makine öğrenmesine dayalı J48, Naive Bayes ve Bayesian Network sınıflandırma algoritmalarını kullanarak belirli bir network trafiğinden elde ettikleri akış verileri üzerinden zombi bilgisayarları etiketleme yönteminden faydalanmışlardır [3]. Fedynshyn ve diğerleri çalışmalarında botnet saldırı tipini belirlemek için sunucu temelli bir uygulama geliştirmişlerdir. Bunun sonucunda tespit edilen atak tipinin IRC, HTTP ya da eşler arası temelli olanlardan hangi gruba dâhil olduğunu bulunup alınacak tedbirlere bu doğrultuda karar verilebilmesi sağlanmıştır [4]. Kandula vd. çalışmalarında Turing testi uygulayarak web sitelerinden ve diğer servislerden gelen saldırıları anında belirleyip, engel olmaya yarayan bir sistemden bahsetmişlerdir[5]. Ramachran vd. tespit ettikleri zombi atakların yöneticilerinin DNS'lerini belirleyip kara listeye almak ve daha sonra bu DNS'lerden gelen veri alımını engellemeye yönelik çalışma yapmışlardır[6] . Bu çalışmada DDoS saldırılarında zombi olarak adlandırılan ve farkında olmadan saldırının parçası olan bilgisayarların, geliştirilen yazılım sistemi sayesinde algılanarak, kullanıcılarının uyarılması ve DDoS atağının engellenmesini sağlayacak güvenlik yönetim sisteminin geliştirilmesi amaçlanmıştır. Bu sayede bireysel kullanıcıların korunmasının yanı sıra toplu DDoS ataklarındaki zombi sayısı düşürülerek,

web tabanlı sistemlere yapılan saldırıların da gücünün düşürülmesi hedeflenmiştir. Bu amaç doğrultusunda oluşturulan veri seti üzerinde makine öğrenmesine dayalı sınıflandırma algoritmaları (Naive Bayes, Karar Ağacı, SVM, Rasgele Orman) kullanılarak istemci bilgisayarın zombi olup olmadığı tespit edilmeye çalışılmıştır.

Bildirinin devamında ikinci bölümünde çalışmada kullanılan yöntemler hakkında bilgi verilmiştir. Üçüncü bölümde, önerilen sistem detaylıca anlatılmıştır. Dördüncü bölümde deneysel veri setleri, değerlendirme kriteri ve elde edilen sonuçlar ele alınmıştır. Beşinci bölümde sonuç üzerinde durulmuş ve gelecek çalışmalardan bahsedilmiştir.

2. Materyal ve Metotlar

2.1 DDoS

Günümüzde en etkili siber ataklardan biri de birçok zombi bilgisayardan oluşan büyük ve koordine edilmiş grup ile hedef sistemin kaynaklarının etkisiz hale getirilmesidir. Bu saldırılar ile başta kimlik ve finansal bilgilerin çalınması gibi birçok zararlı aktivite meydana gelmektedir. Bu tip saldırılardan en bilineni DDoS saldırılarıdır.

DDoS; kullanıcı bilgisayarlarına çeşitli yollarla (Ele geçirilmiş dosyaların içine gömülerek, sosyal mühendislik, mail bombası…) bulaştırılan dosyalar ile (virüs, trojan), zombi durumundaki bilgisayarın internet trafiğini bir web sitesine yönlendirilmesiyle gerçekleşen saldırılardır [1]. Bu saldırılar ile milyonlarca zombi bilgisayar hedef alınan sistemin kaldırabileceği yükün çok üzerinde anlık istek göndererek sistemi cevap veremez hale getirmektedirler.

DDoS saldırılarında zombi bilgisayar tespiti üzerine kullanılan standart yöntemler (güvenlik duvarı, virüs programları vb.) yetersiz kalmakta ve DDoS saldırıları ile zombi bilgisayarların sayısı günden güne artmaktadır. Problemi kökten çözmenin yolu, problemin çıkış kaynağı olan zombi bilgisayarlarda DDoS durumunu tespit etmek, kullanıcıyı uyarmak ve saldırıyı kesmektir.

2.2 Makine Öğrenmesi ve Sınıflandırma

Makine Öğrenmesi, verilen bir problemi problemin bulunduğu ortamdan edinilen veriye göre modelleyen bilgisayar algoritmalarına verilen genel isimlendirmedir [7]. Üzerinde yoğun çalışılan bir alan olduğu için önerilmiş birçok yaklaşım ve algoritma mevcuttur. Bu yaklaşımların bir kısmı tahmin ve kestirim bir kısmı da sınıflandırma yapabilme yeteneğine sahiptir.

Sınıflandırma, sınıfları daha öncede belli olan verilerden yararlanarak (eğitim verisi), sınıfı belli olmayan verileri doğru sınıflara yerleştirmeyi amaçlar [7].

Naive Bayes(NB) sınıflandırma algoritması bir verinin herhangi bir sınıfa ait olma olasılığını tahmin eden istatistiksel bir yöntemdir. Bayes sınıflandırıcılar belirli bir değişkenler grubunun belirli bir sınıfa ait üyelik olasılıklarını tahmin eden istatistiksel sınıflandırıcılardır ve bu sınıflandırma Thomas Bayes'in teoremine dayanmaktadır [8].

Karar ağaçları akış şemalarına benzeyen yapılar olarak tanımlamaktadır. Her bir nitelik bir düğüm tarafından temsil edilir. Dallar ve yapraklar ağaç yapısının elemanlarıdır. En son yapı yaprak, en üst yapı kök ve bunların arasında kalan yapılar ise dal olarak adlandırılmaktadır [9].

Destek vektör makineleri (DVM), temeli istatistiksel öğrenme teorisi olan, yapısal risk minimizasyona dayanan ve çok sayıda bağımsız değişkenle çalışabilen bir sınıflandırıcıdır. DVM algoritması lineer ve lineer olmayan olmak üzere ikiye ayrılmaktadır. Lineer DVM' de veriyi ayırmak için sonsuz sayıda hiperdüzlem oluşturulur ve

tüm bu hiperdüzlemler arasında maksimum-sınırlı hiperdüzlem seçilir. Böylece veri lineer olarak ayrılabilir hale gelir [10].

Rasgele Orman(RO) sınıflandırma yöntemleri, bir sınıflandırıcı yerine birden çok sınıflandırıcı üreten ve sonrasında onların tahminlerinden alınan oylar ile yeni veriyi sınıflandıran öğrenme algoritmalarıdır[11]. Bir dokümanı kategorize etmek için, girdi parametrelerin hepsi ormandaki her bir ayrı ağaca teker teker gönderilir. Ormandaki ağaçların hepsinden dokümanın sınıf etiketi döner ve sonuç olarak en yüksek değere sahip etiket beklenen çıktı olarak seçilir. Başarılı doğruluk oranları vermesi ve büyük veri setleri üzerinde yüksek performanslı çalışması, RO'nun en önemli avantajlarındandır.

Bu çalışmada yukarıda bahsedilen sınıflandırma algoritmalarından yararlanılarak istemci bilgisayarın zombi olup olmadığı tespit edilmeye çalışılmıştır.

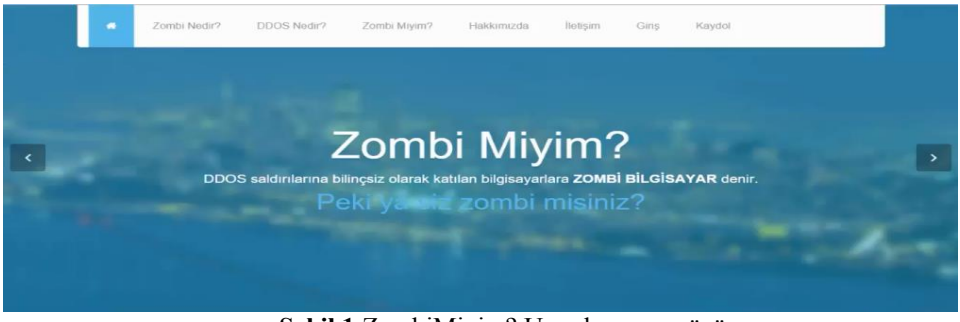
3. Sistem Tasarımı

Çalışmada kullanılan sistem iki temel bileşenden oluşmaktadır: Merkezi web portal ve zombi adayı bilgisayarlarda çalışacak bir yazılım uygulaması.

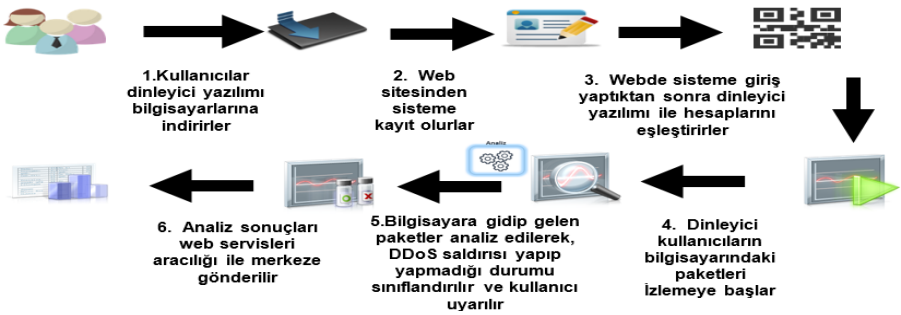
Kullanıcılar ilk olarak merkezi web portalına bağlanarak istemcide çalışacak olan yazılımı bilgisayarlarına indirirler. Daha sonra bu istemci yazılımını kullanarak sisteme kayıt olurlar.

Kurulum ve kayıt aşaması sonrasında güvenlik amacıyla çift taraflı hesap doğrulama işlemini gerçekleştirilir. İstemci yazılım, doğrulama işlemi tamamlandıktan itibaren bilgisayarın internete çıkış trafiğini izlemeye başlar ve makine öğrenmesi tabanlı sınıflandırma algoritmalarını kullanarak trafiğin DDoS olup olmadığını sınıflandırmaya çalışır.
İstemci yazılımı, trafiği izlerken belirli bir adrese, belirli frekanslarda, belirli boyutta veri paketleri gönderilip gönderilmediğini kontrol eder ve sürekli bu bilgileri toplar. Bu aşamada, tüm HTTP (Hypertext Transfer Protocol), TCP (Transmission Control Protocol), UDP (User Datagram Protocol) protokolleri ve dışarıya açılan portlar izlenir. İstemci yazılımı, bu trafik verilerini elindeki güncel öğrenme veri seti üzerinde sınıflandırma algoritmaları kullanarak test eder.

Yazılım, bilgisayarın zombi olduğunu tespit ettiği an bilgisayar sahibine uyarı mesajı gider ve trafiğin kaynağı uygulama bulunup, trafiğin kesilmesini sağlanır. Tespit edilen anormal tüm durumlar; istemci yazılım tarafından, internet üzerinde sunucuda çalışan merkezi yazılıma ve kullanıcı için oluşturulmuş veritabanına kaydedilir. Kullanıcı isterse sisteme bağlanarak, bilgisayarındaki mevcut güvenlik durumunu veya geçmişte oluşan durumları görüntüleyebilir.



Şekil 1 ZombiMiyim? Uygulama arayüzü



Şekil 2 Sistem tasarımı

4. Deneysel Çalışmalar

4.1 Veri Seti

Bu çalışmada kullanılan sınıflandırma algoritmalarını test etmek amacı ile iki adet veri türünden faydalanılmıştır. İlk tür, Celal Bayar Üniversitesi'ne ait 2 ayrı fakültenin (Muradiye ve Turgutlu) ağ çıkış trafikleri izlenerek zombi olmayan ve "NoZ" (No Zombie) olarak etiketlenen verilerin toplanması ile elde edilmiştir. İkinci veri türü, bu çalışma için özel olarak geliştirilen ZombiGen aracı kullanılarak oluşturulan ve "YeZ" (Yes Zombie) olarak etiketlenen zombi verileri içermektedir. Her iki türde veriler toplanıp, birleştirilerek (NoZ + YeZ), 5.000 örnekten oluşan bir veri seti oluşturulmuştur. Veri setindeki her bir örnek için Tablo 1'de bulunan 12 özellik çıkartılmıştır.

Özellik	**Değeri**
IP	Çıkış IP bilgisi
Port	Port bilgisi
PckType	Paket türü (TCP, UDP)
SYN	Flag
ACK	Flag
RST	Flag
PSH	Flag
PKTS	Flow'da gönderilen toplam paket sayısı
BPP	Flow boyunca ortalama paket boyutu
BPS	Paket başına düşen ortalama bit sayısı
PPS	Saniyedeki ortalama paket sayısı
Class	NoZ veya YeZ sınıflandırma bilgisi

Tablo 1 Veri özellik türleri

4.2 Değerlendirme Kriteri

Sınıflandırma algoritmalarının başarı kriterlerinin temeli; doğru ve yanlış sınıfa atanan örnek sayıları ile doğrudan ilişkilidir. Hesaplamalar ise Tablo 2'de görülen hata matrisi olarak adlandırılan bir matrisi temel alır. Hata matrisinde satırlar test kümesindeki örneklere ait gerçek sayıları, kolonlar ise modelin tahmin sonuçlarını ifade etmektedir.

		Tahmin Edilen Sınıf	
		Sınıf=1	Sınıf=0
Gerçek Sınıf	Sınıf=1	TP (True Pozitif)	FN (False Negatif)
	Sınıf=0	FP (False Pozitif)	TN (True Negatif)

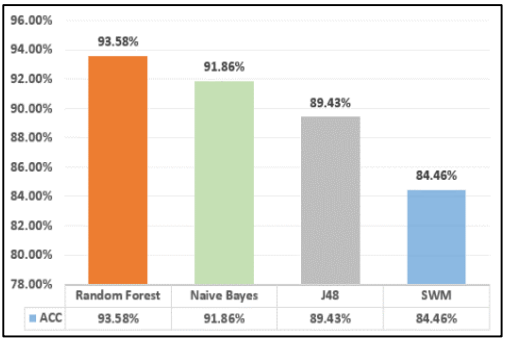
Tablo 2 Hata matrisi

Sınıflandırma algoritmasının başarısının ölçülmesinde kullanılan en popüler ve basit yöntem, modele ait "doğruluk" oranıdır. Formül 1'de görüldüğü gibi Doğru sınıflandırılmış örnek sayısının *(TP +TN)*, toplam örnek sayısına *(TP+TN+FP+FN)* oranıdır.

$$Doğruluk = \frac{(TP+TN)}{(TP+TN+FP+FN)} \qquad Formül\ (1)$$

4.3 Deneysel Sonuçlar

Bu çalışma için oluşturulan veri seti üzerinde zombi bilgisayar tespiti için seçilen sınıflandırma algoritmalarını test etmek amacıyla WEKA yazılım programından yararlanılmıştır. Her Her algoritma, 10 kat çapraz doğrulama testinden geçirilerek, doğruluk oranları aşağıdaki Şekil 3'te özetlenmiştir.



Şekil 3 Sınıflandırma algoritmaları doğruluk oranları

Şekil 3'teki grafik incelendiğinde de açıkça görülmektedir ki ZombiGen aracı ile üretilen "YeZ" etiketli zombi bilgiler ve "NoZ" etiketli zombi olmayan bilgileri içeren veriseti üzerine uygulanan RO, NB, J48 ve DVM algoritmalarından RO en doğru sonucu verirken, DVM en başarısız sonucu vermiştir.

5. Sonuç

İnternet kullanımının yaygınlaşması ile birlikte siber güvenlik gün geçtikçe daha da önem kazanan bir konu haline gelmektedir. Günümüzde internet üzerinden birçok saldırı gerçekleşmekte ve sistemler işlem dışı bırakılmaya yönelik tehditlerle karşı önem kazanan bir konu haline gelmektedir. Günümüzde internet üzerinden birçok saldırı gerçekleşmekte ve sistemler işlem dışı bırakılmaya yönelik tehditlerle karşı karşıya kalmaktadır. Güvenlik önlemi almayan her sistem büyük bir risk altındadır. Bu saldırı yöntemlerinden en etkili ve üzerinde en çok tartışılanlardan biri DDoS'dur. Bu çalışma ile DDoS saldırılarında zombi olarak adlandırılan ve farkında olmadan saldırının parçası olan bilgisayarların, geliştirilen yazılım sistemi sayesinde algılanarak, kullanıcılarının uyarılması ve DDoS atağının engellenmesini sağlayacak güvenlik yönetim sisteminin geliştirilmesi amaçlanmıştır. Bu sayede bireysel kullanıcıların korunmasının yanı sıra toplu DDoS ataklarındaki zombi sayısı düşürülerek, web tabanlı sistemlere yapılan saldırıların da gücünün düşürülmesi hedeflenmiştir. Saldırıları belirlemek amacını gerçekleştirirken makine öğrenmesine dayalı sınıflandırma algoritmalarından faydalanılmıştır. Bu algoritmalar içerisinde en başarılı sonuçların RO sınıflandırıcı ile elde edildiği gözlemlenmiştir.

Kaynaklar

[1] Wikipedia bilgi sayfası, DDos, http://tr.wikipedia.org/wiki/DDoS, Erişim tarihi: 20 Ekim 2015

[2] eSecurity Planet, 5 tips for Fighting DDoS Attacks, http://www.esecurityplanet.com/network-security/5-tips-for-fighting-DDoS-attacks.html, Erişim tarihi: 18 Eylül 2015

[3] Livadas, C., Walsh, R., Lapsley, W. ve Strayer, T. "Using machine learning techniques to identify botnet traffic", Proceeding of Local Computer Network, 2006.

[4] Fedynyshyn, G., Chuah, M.C. ve Tan, G. "Detection and classification of different botnet C&C channels", Proceedings of the 8th International Conference on Autonomic and Trusted Computing, ss. 228-242, 2011.

[5] Kandula, K. vd. "Botz-4-Sale: surviving organized DDoS attacks that mimic flash

crowds", NSDI '05: 2nd Symposium on Networked Systems Design & Implementation, 2005.

[6] Ramachandran, A. ve Feamster, A. "Understanding the network-level behavior of spammers", Technical Report GT-CSS-2006-001, Georgia Tech, Feb. 2006.

[7] Tsiptsis, K. ve Chorianopoulos, A. "Data mining techniques in CRM: Inside customer segmentation", Wiley Publishing, United Kingdom, 2010.

[8] Han, J. ve Kamber, M. "Data Mining Concepts and Techniques", 2nd Ed., Morgan Kaufmann Publishers, Massachusetts, 2006.

[9] Quinlan, J.R. "C4.5: Programs for machine learning", Morgan Kaufmann Publishers, Massachusetts, 1993.

[10] Aha D.W, Kibler D. ve Albert M.K. "Instance-based learning algorithms", Machine Learning, 6(1): 37-66, 1991.

[11] Akar, Ö. ve Güngör, G. "Rastgele orman algoritması kullanılarak çok bantlı görüntülerin sınıflandırılması", Jeodezi ve Jeoinformasyon Dergisi, ss. 139-146, 2012.