



**WEB SAYFALARINDA KULLANILAN GÜVENLİK KODU SEÇİMİNE
YÖNELİK BİR ARAYÜZ GELİŞTİRİLMESİ**

Necla ULUHATUN

**YÜKSEK LİSAN TEZİ
ADLI BİLİŞİM ANA BİLİM DALI**

**GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ**

ARALIK 2019

Necle ULUHATUN tarafından hazırlanan “WEB SAYFALARINDA KULLANILAN GÜVENLİK KODU SEÇİMİNE YÖNELİK BİR ARAYÜZ GELİŞTİRİLMESİ” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Adli Bilişim Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Dr. Öğr. Üyesi Hüseyin ÇAKIR
Bilgisayar ve Öğretim Teknolojisi, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

.....

Başkan: Prof. Dr. Refik SAMET
Bilgisayar Mühendisliği, Ankara Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

.....

Üye: Prof. Dr. Ömer Faruk BAY
Elektrik Elektronik Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

.....

Tez Savunma Tarihi: 19/12/2019

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

.....

Unvan Ad SOYAD
Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- 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 çalışmada 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.

İmza

Necla ULUHATUN
09/01/2020

WEB SAYFALARINDA KULLANILAN GÜVENLİK KODU SEÇİMİNE YÖNELİK BİR ARAYÜZ GELİŞTİRİLMESİ

(Yüksek Lisans Tezi)

Necla ULUHATUN

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

Aralık 2019

ÖZET

Teknoloji ve internetin hızla ilerlemesiyle birlikte siber suçlar giderek artmaktadır. Captcha bu suçları engellemek amacıyla oluşturulan bir güvenlik katmanı olarak kullanılmaktadır. Captcha, sisteme giriş yapıldığında girişin kullanıcı tarafından yapıp yapılmadığının ayırt edilebilmesi için tasarlanmış bir güvenlik mekanizmasıdır. Captcha, verilere erişimin gerçek kişilerle sağlamak ve web güvenliğini artırmak amacıyla kullanılmaktadır. Captcha ile ilgili pek çok çalışma yapılmıştır. Bunlar daha çok Captcha hakkında genel inceleme, yeni bir model oluşturma ve mevcut modellere siber saldırı yaparak sisteme izinsiz giriş yapmakla ilgilidir. Bu çalışma literatür taramasında elde edilen çalışmalardan farklı olarak, en uygun ve güvenilir Captcha amaçlaması bakımından özgündür. Bu çalışmanın amacı, web güvenliğine yönelik analiz ve inceleme sonuçlarına dayanarak, en güvenilir Captcha modeli ve katmanının hangisi olması gerektiği ve site amacına göre en çok tercih edilen Captcha hangisi olduğunu belirlemektir. Yapılan çalışmada; Türkiye’de arama motorlarında en üst sırada çıkan, Alexa istatistiği ve uzman görüşü alınarak web siteleri gruplandırılmıştır. Gruplandırılmış veri kümeleri belli bir frekans yüzdesi ile taranmıştır. İnceleme ve tarama sonucunda web sitelerden elde edilen bulguların yorumlanması ve çözümlenmesi yapılmıştır. Bulguların analizi sonucunda; kural tabanlı etkili bir captcha seçim algoritması hazırlanmıştır. Bu algoritma ile web güvenliği; sitelerin kullanım amacı, zamandan tasarruf etme, zorluk seviyesi ve kırılma oranlarına göre seçimler sunarak site güvenliği sağlayan site kurucularına etkili seçenekler sunan bir web sitesi geliştirilmiştir.

Bilim Kodu : 92412

Anahtar Kelimeler : Kural tabanlı mantık, güvenlik kodu, web sayfalarında güvenlik, kötücül yazılımlar, siber suç, spam, giriş sistemi ve doğrulama sistemleri

Sayfa Adedi : 119

Danışman : Dr. Öğr. Üyesi Hüseyin ÇAKIR

DEVELOPING AN INTERFACE FOR CAPTCHA SELECTION IN
WEB PAGES

(M. Sc. Thesis)

Necla ULUHATUN

GAZİ UNIVERSITY
INFORMATICS INSTITUTE

December 2019

ABSTRACT

Cybercrime is increasing with the rapid advance of technology and internet. Captcha is used as a security layer created to prevent these crimes. Captcha is a security mechanism designed to distinguish whether the entry is made by the user when logging into the system. Captcha is used to provide access to data with real people and to increase web security. Many studies have been made on captcha. These studies are more about Captcha's general review, creating a new model and cyber attack on existing models, and unauthorized access to the system. This study differs from the studies obtained in the literature review in terms of the most appropriate and reliable Captcha aim. The aim of this study is to determine which of the most reliable Captcha models and layers should be based on the results of the analysis and examination of web security and which is the most preferred Captcha according to the purpose of the site. In the study; In the top row of the search engines in Turkey, Alexa statistics and expert opinion on the website are grouped. The grouped datasets were scanned with a certain percentage of frequency. Interpretation and analysis of the findings obtained from the web sites as a result of the review and screening were conducted. As a result of the analysis of the findings; An effective captcha selection algorithm based on rule base logic is prepared. Web security with this algorithm; The site provides effective options for site builders who provide site security by making choices based on their intended use, time savings, difficulty levels and break rates.

Science Code : 92412

Key Words : Rule base logic, captcha, security in web pages, malware, cybercrime, spam, entry system and turing test

Page Number : 119

Supervisor : Dr. Öğr. Üyesi Hüseyin ÇAKIR

TEŞEKKÜR

Bu tezin planlanmasında ve hazırlanmasında zaman ayırarak ilgi ve desteğini esirgemeyen, bilgi ve tecrübesi ile çalışmamı yönlendiren, verdiği öneri, yorum ve düzeltmelerle önemli destek sağlayan tez danışmanım Hüseyin ÇAKIR'a; araştırma aşamasında sağladıkları bilgi ve dokümanlar için Sn. Fatma ALTINIŞIK, Burcu BOZKURT ve Gökhan GÜMÜŞ'e; tez hazırlama süresince desteklerini esirgemeyen Yazılım Geliştirme Müdürlüğü ve Güvenlik Yönetim Şube'deki çalışma arkadaşlarıma; ayrıca her daim maddi ve manevi yardımlarını esirgemeyen, her koşulda yanımda olan anneme, babama ve kardeşlerime teşekkürlerimi sunarım.



İÇİNDEKİLER

	Sayfa
ÖZET	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
İÇİNDEKİLER	vii
ÇİZELGELERİN LİSTESİ.....	ix
ŞEKİLLERİN LİSTESİ	xi
SİMGELER VE KISALTMALAR	xiii
1. GİRİŞ.....	1
2. CAPTCHA VE CAPTCHA ÇEŞİTLERİ.....	5
2.1. Captcha Tanımı	7
2.2. Captcha Katmanları.....	8
2.2.1. Tek katmanlı	8
2.2.2. İki katmanlı	10
2.3. Captcha Gelişimi ve Türleri	10
2.3.1. Basit captcha	11
2.3.2. Güncel captcha.....	11
2.3.3. Matematik captcha.....	11
2.3.4. Karmaşık captcha.....	12
2.3.5. Nesneli captcha	12
2.3.6. Resim captcha	13
2.3.7. Slider captcha.....	14
2.3.8. ReCaptcha captcha	15
2.4. Captcha Genel Mantığı ve İşleyişi	16
2.5. DeCaptcha Adımları	16
2.6. Captcha Yakın Geleceği	20
2.7. Kullanım Alanları	24
2.7.1. Web site üyeliklerini kontrol etmek	24
2.7.2. E-mail adreslerini gizlemek	25
2.7.3. Bloglara spam gönderilmesini önlemek	25
2.7.4. Anketler	26
2.7.5. Worm ve spamlardan korunmak.....	26
2.7.6. Arama motorları.....	26
2.8. Güvenliği Sağlamadaki Rolü	26
3. LİTERATÜR DEĞERLENDİRİLMESİ	29
4. YÖNTEM.....	41
4.1. Çalışma Kümeleri.....	41
4.2. Verilerin Toplanması	42
4.3. Verilerin Çözümlemesi ve Yorumlanması	49
4.4. Kural Tabanlı Algoritmanın Oluşturulması.....	51
4.5. Web Arayüz Geliştirilmesi	60

	Sayfa
5. BULGULAR VE YORUM	69
5.1. Captchaların Kırılma Oranlarına Göre İncelenmesi	69
5.2. Web Site Amacına Göre Captchaların İncelenmesi.....	70
5.2.1. Arama motorları.....	70
5.2.2. Sosyal medya siteleri	72
5.2.3. Haber siteleri	74
5.2.4. E-ticaret siteleri	77
5.2.5. İlan siteleri.....	79
5.2.6. Finansal kurum siteleri	81
5.2.7. Kişisel siteler ve bloglar	84
5.2.8. Eğitim siteleri	84
5.2.9. Firma siteleri	89
5.2.10. Sağlık siteleri.....	90
5.2.11. Kamu kurumu siteleri	94
5.2.12. Anket siteleri	95
5.2.13. Eğlence siteleri.....	96
5.2.14. Sanatsal siteler	99
5.2.15. Portal siteler	100
5.2.16. E-posta servis sağlayıcı siteler	102
5.3. İncelenen Web Sitelerinde Captcha Genel Kullanımı	103
5.4. Web Sitelerinde Captcha Türü Kullanım Durum İncelenmesi.....	103
5.5. Web Site Amacına Göre Captcha Katman İncelenmesi	104
5.6. Web Site Amacına Göre Captcha Kullanım İstatistiği	105
5.7. Web Site Kullanım Amacına En Uygun Kural Tabanlı Captcha Algoritması Oluşturma.....	106
6. SONUÇ VE ÖNERİLER	111
KAYNAKLAR.....	115
ÖZGEÇMİŞ	119

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 4.1. Captcha kullanım sayısı.....	41
Çizelge 4.2. Web site kullanım amacı.....	41
Çizelge 4.3. Kullanılan captchalar.....	42
Çizelge 4.4. Kullanılan captcha katmanı	42
Çizelge 4.5. Özet çizelge.....	50
Çizelge 4.6. Algoritma adımları	59
Çizelge 5.1. Captcha katmanlarında kırılmaların karşılaştırması.....	69
Çizelge 5.2. Captcha türünde kırılmaların karşılaştırması.....	70
Çizelge 5.3. Arama motorları	71
Çizelge 5.4. Sosyal medya siteleri	73
Çizelge 5.5. Yerel haber siteleri.....	74
Çizelge 5.6. Ulusal haber siteleri.....	75
Çizelge 5.7. Uluslararası haber siteleri	76
Çizelge 5.8. B2B siteleri	77
Çizelge 5.9. B2C siteleri	78
Çizelge 5.10. C2C siteleri	79
Çizelge 5.11. İlan siteleri	80
Çizelge 5.12. Banka siteleri	81
Çizelge 5.13. Borsa siteleri	82
Çizelge 5.14. Kripto para siteleri	83
Çizelge 5.15. Kişisel siteler ve bloglar.....	84
Çizelge 5.16. Okul siteleri.....	85
Çizelge 5.17. Üniversite siteleri.....	86
Çizelge 5.18. Dershane siteleri	87
Çizelge 5.19. Uzaktan eğitim siteleri	88
Çizelge 5.20. Yayınevi siteleri.....	89
Çizelge 5.21. Firma siteleri	90
Çizelge 5.22. E-randevu siteleri.....	91
Çizelge 5.23. E-tahlil sonuç siteleri.....	92
Çizelge 5.24. Hastane siteleri.....	93
Çizelge 5.25. Eczane siteleri	94
Çizelge 5.26. Kamu kurum siteleri	95

Çizelge	Sayfa
Çizelge 5.27. Anket siteleri.....	96
Çizelge 5.28. Oyun siteleri.....	97
Çizelge 5.29. Bahis siteleri	98
Çizelge 5.30. Gezi siteleri	99
Çizelge 5.31. Sanatsal siteleri	100
Çizelge 5.32. Portal siteleri	101
Çizelge 5.33. E-posta servis sağlayıcı siteleri.....	102
Çizelge 5.34. Captcha kullanım durumu.....	103
Çizelge 5.35. Captcha çeşitliliğinde kullanım	103
Çizelge 5.36. Captcha kullanım amacına göre çeşitliliği.....	104
Çizelge 5.37. Amaca göre captcha kullanımı	105
Çizelge 5.38. Captcha katmanlarında güvenlik düzeyi.....	106
Çizelge 5.39. Captcha çeşitlerinde güvenlik düzeyi	107
Çizelge 5.40. Captcha katmanlarında kullanım sıklığı.....	107
Çizelge 5.41. Captcha çeşitlerinde kullanım sıklığı.....	108
Çizelge 5.42. Site amacına göre captcha kullanım sıklığı	108

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 2.1. Turing test.....	5
Şekil 2.2. Karmaşıklık, rotasyonu ve gürültüsü artırılmış güvenlik kodları.....	7
Şekil 2.3. Basit captcha.....	11
Şekil 2.4. Güncel captcha.....	11
Şekil 2.5. Matematik captcha.....	12
Şekil 2.6. Karmaşık captcha.....	12
Şekil 2.7. Nesneli captcha.....	13
Şekil 2.8. Resim captcha.....	14
Şekil 2.9. Slider captcha.....	14
Şekil 2.10. reCaptcha	15
Şekil 2.11. Captcha tanıma	17
Şekil 2.12. Captcha kırma temel adımları.....	19
Şekil 2.13. Captcha kırma şeması	20
Şekil 2.14. Çizim captcha	21
Şekil 2.15. Hareket captcha	21
Şekil 2.16. 3D captcha	22
Şekil 2.17. Key captcha	22
Şekil 2.18. PlayThru captcha	22
Şekil 2.19. reCaptcha	23
Şekil 2.20. Invisible reCaptcha	24
Şekil 3.1. Literatür taraması(a)	38
Şekil 3.2. Literatür taraması(b)	39
Şekil 3.3. Literatür taraması(c)	39
Şekil 4.1. Verilerin toplanması	43
Şekil 4.2. ReCaptcha veri toplanması	43
Şekil 4.3. Captchasız siteden veri toplanması.....	44
Şekil 4.4. Slider captcha veri toplanması-1	45
Şekil 4.5. Slider captcha veri toplanması-2	45
Şekil 4.6. Karmaşık captcha veri toplanması.....	46
Şekil 4.7. Matematik captcha veri toplanması	46
Şekil 4.8. Basit captcha veri toplanması	47

Şekil	Sayfa
Şekil 4.9. Ses tabanlı captcha veri toplanması	47
Şekil 4.10. Güncel captcha veri toplanması	48
Şekil 4.11. Resim captcha veri toplanması	49
Şekil 4.12. Klasik küme mantık	51
Şekil 4.13. Kural tabanlı küme mantık	52
Şekil 4.14. Klasik ve kural tabanlı küme mantık	52
Şekil 4.15. Katman güvenlik seviyesi	53
Şekil 4.16. Captcha güvenlik seviyesi	54
Şekil 4.17. Katman popülerlik seviyesi	54
Şekil 4.18. Captcha popülerlik seviyesi	55
Şekil 4.19. Kullanım amacına göre seviyelendirme	56
Şekil 4.20. Algoritma sınıfları	57
Şekil 4.21. Akış diyagramı	58
Şekil 4.22. Captcha anasayfa(a)	60
Şekil 4.23. Captcha anasayfa(b)	61
Şekil 4.24. Captcha anasayfa(c)	62
Şekil 4.25. Captcha anasayfa(d)	63
Şekil 4.26. Captcha anasayfa(e)	64
Şekil 4.27. Captcha anasayfa(f)	65
Şekil 4.28. Captcha anasayfa(g)	66
Şekil 4.29. Captcha anasayfa(h)	67
Şekil 4.30. Captcha anasayfa(i)	68

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler

%

Yüzde

f

Frekans

Açıklamalar

Kısaltmalar

OCR

Optik karakter okuyucu

CAPTCHA

İnsan ve bilgisayar ayrımı amaçlı tam otomatik genel turing testi

RGB

Red green blue

AI

Artificial intelligence

3D

3 dimension

HTML5

Hyper text markup language

IP

Internet protocol

WWW

World wide web

BOT

Robot

URL

Uniform resource locator

CaRP

Captcha

NOR

Not or

NAND

Not and

ALEXA

Web ölçümlendirme

DB

Data base

B2B

Business to business

B2C

Business to customer

C2C

Customer to customer

GSM

Global System for Mobile Communications

TBMM

Türkiye Büyük Millet Meclisi

YÖK

Yüksek Öğretim Kurumu

TÜBİTAK

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

İŞKUR

Türkiye İş Kurumu

TRT

Türkiye Radyo Televizyon Kurumu Yasası

EGM

Emniyet Genel Müdürlüğü

MEB

Milli Eğitim Bakanlığı

BTK

Bilgi Teknolojileri ve İletişim Kurumu

MSN

Microsoft Network

GMAIL

Google Mail

1. GİRİŞ

Bu bölümde araştırmanın problemi açıklanarak amacı, önemi, varsayımları ve sınırlılıklarına yer verilmiş; araştırmada geçen bazı kavramların tanımları üzerinde durulmuştur.

Problem Durumu/Konunun Tanımı

Günümüz internet yaşamında günden güne baş döndürücü şekilde gelişen teknolojik gelişmeler neticesinde internet güvenliği birçok problemle karşı karşıyadır. Bunlardan birisi de web sitelerinde insan ya da bot (kötücül siber yazılım) ayırımı yapmaktır. Bot saldırıları (kötücül siber saldırıları) ile internet dünyası siber saldırılar ile karşı karşıyadır ve bu durum maddi, manevi, özel hakların gizliliği, emek ve zaman kaybı gibi pek çok istenmedik sonuçlar ortaya çıkarmaktadır. Bu tür sonuçların ortaya çıkmaması için özellikle web site kurucuların site güvenliğini dış saldırılara karşı koruması gerekmektedir.

İnternet teknolojilerinin gelişmesi ve kullanımının yaygınlaşmasıyla, bu sistemlerin güvenliği konusu da önemli bir unsur haline gelmiştir. Güvenlik amaçlı oluşumlar geliştirildiği gibi bunlara karşıt sistem açıklarının üzerine giden kötücül yazılımlar da ortaya çıkmıştır. Bu bot saldırılarının (kötücül siber saldırılar) önüne geçebilmek için doğrulama sistemlerine ihtiyaç duyulmuştur.

Araştırmanın Amacı

Araştırmanın genel amacı, Türkiye’de kullanılan web sitelerinde, siber saldırılara karşı korunma sağlayan Captcha kullanım oranlarını, bu Captcha çeşitlerini ve Captcha kırılma oranlarını inceleyerek sitelerin saldırılara karşı korunmada eksik kalan yönlerini belirlemektir. Bu kapsamda; saldırılara karşı korunmada web siteleri kullanım amaçlarına yönelik geliştirilen kural tabanı (rule base logic) algoritmasına dayalı en uygun Captcha kullanımını belirlemektir.

Bu genel amaca ulaşabilmek için alt amaçlar belirlenmiştir;

1. Güvenlik kodları (Captchalar) kırılma oranlarına göre farklılık göstermekte midir?
2. Web siteleri kullanım amaçlarına göre Captcha kullanımı farklılık göstermekte midir?
3. İncelenen Web sitelerinde Captcha genel kullanımı farklılık göstermekte midir?

4. Web sitelerinde Captcha kullanım çeşitliliğine göre farklılık göstermekte midir?
5. Web sitelerin kullanım amaçlarına göre Captcha katmanı farklılık göstermekte midir?
6. Web sitelerin kullanım amacına göre Captcha kullanım istatistiği farklılık göstermekte midir?
7. Web siteleri kullanım amaçlarına yönelik geliştirilen kural tabanı (rule base logic) algoritması nasıl olmalıdır?

Araştırmanın Önemi

Araştırmanın önemi, site geliştiricilerine dışardan ya da içerden web sitelerine yapılacak herhangi bir siber saldırıya karşı güvenliğin sağlanması için uygun bir Captcha önermektedir. Böylece site geliştiricilerinde Captcha kullanılmasının ehemmiyeti konusunda farkındalık sağlamaktır.

Türkiye’de kullanımda olan web sitelerini kullanım amaçlarına göre gruplandırılarak, Captcha kullanım oranları belirlemek ve bu çerçevede güvenilirlik seviyelerini ortaya dökmektir. Bu kapsamda; daha güvenilir bir Captcha modeli tercih edilebilmesi, araştırmanın sayısal sonuçlarına göre tasarlanan kural tabanlı algoritması geliştirmektir. Böylece Captcha model geliştiricilerine kullanıcı dostu ve güvenilir bir algoritma önerilmektedir.

Sınırlılıklar

Araştırma;

1. Türkiye internet sınırları içerisinde erişilebilen web siteleri ile,
2. Arama motorlarında üst dizinde çıkan ve Alexa ile en üst sıralardaki siteler ile,
3. Sitelerin kullanım amaçlarına göre on altı grupta (Arama Motorları, Sosyal Medya Siteleri, Haber Siteleri, E-Ticaret Siteleri, İlan Siteleri, Finansal Kurum Siteleri, Kişisel Siteler ve Bloglar, Eğitim Siteleri, Firma Siteleri, Sağlık Siteleri, Kamu Kurum Siteleri, Anket Siteleri, Eğlence Siteleri, Sanatsal Siteler, Portal Siteleri, E-Posta Servis Sağlayıcı Siteler),
4. Captcha’da kullanılan üç katmanla (Metin Tabanlı, Resim Tabanlı, Ses Tabanlı),

5. Captcha en çok tercih edilen sekiz çeşidiyle (Basit Captcha, Güncel Captcha, Matematik Captcha, Karmaşık Captcha, Nesneli Captcha, Resim Captcha, Slider Captcha, reCaptcha),
 6. 236 tanesi Captcha içeren ve 104 tanesi Captcha içermeyen toplam 340 web sitesi ile,
- sınırlıdır.

Tanımlar

Turing Test: Turing Testinin amacı bir bilgisayarın düşündüğünü söyleyebilmenin mümkün olup olamayacağıdır. Turing testine göre sorgulayıcının soru sorması suretiyle, yöneltilen sorulara cevap verenlerden hangisinin bilgisayar hangisinin insan olduğunu saptamaya çalışmasıdır. Sorgulayıcının soruları sadece bir klavye aracılığıyla yazılarak gönderilmektedir. Tekrarlanan testler sonucunda sorgulayıcı, cevap vericinin insan olup olmadığını saptayamadığı takdirde bilgisayar Turing Testini geçmiş sayılmaktadır (James, 2001).

Captcha: Güvenlik kodu (Captcha-Completely Automated Public Turing test to tell Computers and Humans Apart) otomatik kayıt, spam veya kötü amaçlı bot programlarını önlemek için kullanılır (VonAhn, Blum, Hopper ve Langford, 2003; VonAhn, Blum, Hopper ve Langford, 2004). İnsanlar için kolay ama bilgisayarlar için çözülmesi zor olan otomatik bir test üretir ve değerlendirir. Bir Captcha'nın insan tarafından çözülmesi oranı %90 veya üssü iken bilgisayar programları için yalnızca %1'den daha düşük bir orana ulaşırsa Captcha güvenli olarak kabul edilmektedir (Bursztein, Martin ve Mitchell, 2011).

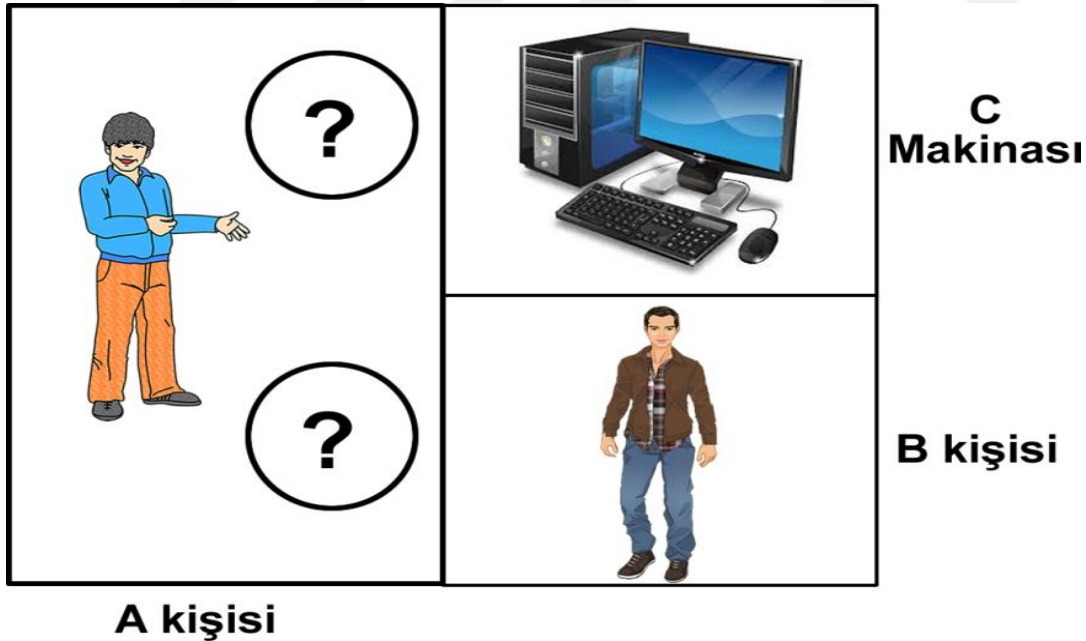
Kural Tabanı: Standart küme kuramında herhangi bir nesne bir kümeye ya aittir ya da değildir. Bunun ortası yoktur. Ayrıca bu iki kümeden hiçbirine ait olmaması söz konusu değildir. Bu ilke bir nesnenin aynı anda hem bir şey olması hem de o şey olmaması çelişkisini olanaksız kılmaktadır. Kural tabanlıda, elemanlar bir kümeye ancak kısmen aittir. Ayrıca, aynı anda birden çok kümeye de ait olabilirler (Alicı ve Karatepe, 2002).

2. CAPTCHA VE CAPTCHA ÇEŞİTLERİ

Siber dünyada, teknoloji ve internetin hızla ilerlemesi beraberinde gelişmekte olan siber suçları da getirmektedir. Captcha Çeşitliliği bu suçları engellemek amacıyla oluşturulan bir güvenlik katmanı olarak bilinir.

Turing Test

İlk olarak 1950 yılında Alan Turing Computing Machinery and Intelligence isimli makalesinde değinmiştir. Turing Testinin amacı bir bilgisayarın düşündüğünü söyleyebilmenin mümkün olup olmayacağıdır. Turing testine göre sorgulayıcının soru sorması suretiyle, yöneltilen sorulara cevap verenlerden hangisinin bilgisayar hangisinin insan olduğunu saptamaya çalışmasıdır. Sorgulayıcının soruları sadece bir klavye aracılığıyla yazılarak gönderilmektedir. Tekrarlanan testler sonucunda sorgulayıcı, cevap vericinin insan olup olmadığını saptayamadığı takdirde bilgisayar Turing Testini geçmiş sayılmaktadır (James, 2001). Şekil 2.1’de Turing test mantığı gösterilmiştir (McDermott, 2014; Çakır ve Ulubatun,2018).



Şekil 2.1. Turing test (Çakır ve Ulubatun, 2018)

Güvenlik kodu (Captcha-Completely Automated Public Turing test to tell Computers and Humans Apart) otomatik kayıt, spame-mail (istenmeyen posta) veya kötü amaçlı bot programlarını önlemek için kullanılır (VonAhn, Blum, Hopper ve Langford, 2003; VonAhn,

Blum, Hopper ve Langford, 2004). İnsanlar için kolay ama bilgisayarlar için çözümlenmesi zor olan otomatik bir test üretir ve değerlendirir. Bir Captcha'nın insan tarafından çözülmesi oranı %90 veya üssü iken bilgisayar programları için yalnızca %1'den daha düşük bir orana ulaşırsa Captchagüvenli olarak kabul edilmektedir (Bursztein, Martin ve Mitchell, 2011; Çakır ve Ulubatun,2018).

Captcha, web ortamında formlara giriş yaparken, mesaj atarken, şifre geri alırken ya da bir siteye üye olurken, kısaca günlük internet kullanımı sırasında birçok yerde karşılaşılan kargacık burgacık, farklı tekniklerle okunması zorlaştırılan ve insan ile botları (kötücül siber yazılımları) ayırt etmek için geliştirilen bir projedir. Projenin asıl amacı web ortamında insanlar ile bilgisayar arasındaki davranışların fark edilmesidir (Captcha,2017).

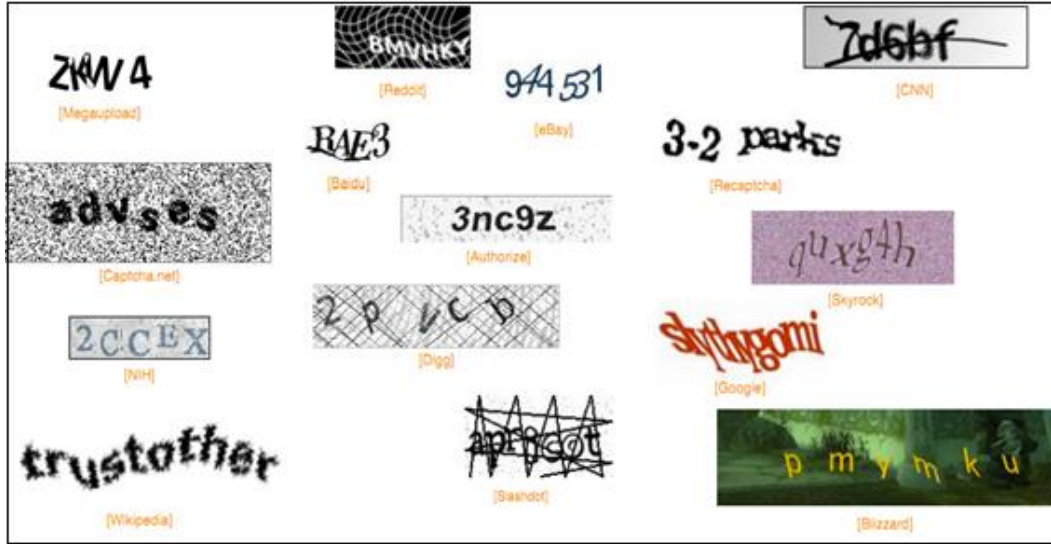
Bu doğrulama uygulaması olmaksızın saldırgan(spammer) kişilerin hedef seçtikleri sistemlere zarar vermeleri, şifre kurtarma formlarında kaba kuvvet(brute force) saldırısı kullanarak şifre kırmak, botların mesaj formlarında reklam ya da zararlı linklerin paylaşımları çok çok daha kolaydı. Bu durumların önüne geçilebilmesi için okunması zor, eğri, yamuk, farklı renklerde ya da farklı yöntemlerle deforme edilmiş halde, kısaca resim işleme araçları ile botların tanımlayamayacağı ve sadece insanların ayırt edebileceği ve geçebileceği düşünülen bu doğrulama uygulamaları kullanılmaya başlanmıştır (Çakır ve Ulubatun, 2018).

Captcha güvenliği ve tasarımı ile ilgili birçok çalışma grubu tarafından incelenmiştir (Luis, Maurer, McMillen, Abraham ve Blum, 2008; Ahn, Blum, Hopper ve Langford, 2003; Gao, Tang, Liu,2017; (Eken, Sayar,2 015); Demirel, Kılıç,2011). Mevcut Güvenlik kodları (Captcha) metin tabanlı, görüntü tabanlı ve ses tabanlı olarak üç kategoriye ayrılabilir. Metin tabanlı Captcha genellikle İngilizce harfler ve Arapça rakamlara dayanır ve bir makinenin tanınmasını önlemek için karmaşık çarpıklık (sophisticated distortion), rotasyon (rotation) veya gürültü paraziti (noiseinterference) kullanır (Çakır ve Ulubatun, 2018).

Karmaşık çarpıklık: Metin tabanlı Captcha'da tanımlanması istenen karakterlerin kompleks bir yapıda içe geçmiş olması durumudur.

Rotasyon: Metin tabanlı Captcha'daki karakterlerin açıkça döndürülmüş ve her karakterin dönüş açısı farklı olması durumudur (Çakır ve Ulubatun, 2018).

Gürültü paraziti: Metin tabanlı Captcha karakterlerinde veya karaktere komşu piksellerde bulunan istenmeyen ve OCR istemlerde okumayı zorlaştıran karakter ile aynı veya farklı renklerdeki piksellerin eklenmesidir.



Şekil 2.2. Karmaşıklığı, rotasyonu ve gürültüsü artırılmış güvenlik kodları

(Hugomdq, 2018)

Görüntü tabanlı ve ses tabanlı Captcha kategorisine kıyasla, metin tabanlı Captcha en yaygın kullanılan şemadır (Yan ve El Ahmad, 2008). Bu yaygın kullanım, belirgin avantajlarından kaynaklanmaktadır (Chellapilla, Larson, Simard ve Czerwinski, 2005; Kumar, Kevin, Patrice ve Mary, 2005) ayrıca metin tabanlı Captcha, Güvenlik kodlarının (Captcha) en eski formudur ve insanlar diğer formlara kıyasla metin tabanlı Captcha tercih etmeye daha eğilimlidirler (Çakır ve Uluhatun, 2018).

2.1. Captcha Tanımı

Bir sisteme giriş yapıldığında girişin kullanıcı tarafından mı yoksa bilir kötücül amaçlı bir bilgisayar yazılımı tarafından mı yapılmadığını ayırt edebilmek için tasarlanmış bir güvenlik mekanizması ve kötü niyetli bilgisayar programlarına karşı korunma amaçlı olarak kullanılır. Bu nedenle girişin insan mı yoksa kötücül bilgisayar yazılımı tarafından mı yapıldığı belirlenmiş olur ve bu sistemlere erişim için önem arz etmektedir.

2.2.Captcha Katmanları

Güvenlik kodu (Captcha, İnsan ve Bilgisayar Ayrımı Amaçlı Tam Otomatik Genel Turing Testi) otomatik kayıt, spam veya kötü amaçlı bot programlarını önlemek için kullanılır.

İnsanlar için kolay ama bilgisayarlar için çözmesi zor olan otomatik bir test üretir ve değerlendirir.

Bir Captcha insanlar için çözülme oranı %90 veya üssü iken bilgisayar programları için yalnızca %1'den daha düşük bir orana ulaşırsa Captcha güvenli olarak kabul edilir (Çakır ve Uluhatun, 2018).

Captcha temelde tek katmanlı ve iki katmanlı olarak iki ana katmana ayrılmıştır:

2.2.1. Tek katmanlı

Tek katmanlı Güvenlik kodları (Captcha) metin tabanlı, görüntü tabanlı ve ses tabanlı olarak üç kategoriye ayrılabilir.

Metin tabanlı

Metin tabanlı Güvenlik kodları (Captcha) genellikle İngilizce harfler ve Arapça rakamlara dayanır ve bir makinenin tanınmasını önlemek için karmaşık çarpıklık, rotasyon veya gürültü paraziti kullanır. Son iki Güvenlik kodları (Captcha) kategorisine kıyasla, metin tabanlı Güvenlik kodları (Captcha) en yaygın kullanılan şemadır. Bu yaygın kullanım, belirgin avantajlarından kaynaklanmaktadır. Dünya çapında kullanıcılar için sezgisel olan problem metni tanımadır. Genel olarak, insanlar İngilizce harfleri ve Arapça rakamları tanıyabilir, bundan dolayı metin tabanlı Captcha'nın yerleştirme sorunları azdır; ayrıca metin tabanlı Güvenlik kodları (Captcha), Güvenlik kodların (Captcha) en eski formudur ve insanlar diğer formlara kıyasla metin tabanlı Güvenlik kodları (Captcha) tercih etmeye daha eğilimlidirler (Çakır ve Uluhatun, 2018).

Güvenlik, metin tabanlı Güvenlik kodlar (Captcha) için en önemli konudur. Captcha başarısızlığına ilişkin çok sayıda örnek var ve bu konuda birçok saldırı tespit edilmiştir. Son zamanlarda yapılan araştırmalar; basit ve genel atakların, çok çeşitli metin tabanlı Güvenlik kodları (Captcha), tek adımda kırıldığını iddia etmekte. Birçok metin tabanlı Güvenlik kodların (Captcha) güvensiz olduğu kanıtlanmış olmasına rağmen, en son yapılan çalışmalar Güvenlik kodlarının (Captcha) hala yaygın olarak kullanılan bir güvenlik mekanizması olduğu ve metin tabanlı Güvenlik kodların (Captcha) güvenliği akademik alanda hala çok değinilen bir konudur (Çakır ve Uluhatun, 2018).

Resim tabanlı

Yazılım geliştiriciler çoğunlukla bot ve spam saldırılarından korunmak için Captcha kullanmaktadır. Fakat sürekli gelişen teknoloji ile birlikte güvenliği sağlamak için yeniliğe ayak uydurmak gerekmektedir. Captcha da gelişime ayak uydurmak için sürekli gelişim halindedir. Optik karakter okuyucu (Optical Character Recognition-OCR) sistemler artık metin tabanlı Güvenlik kodlarını (Captcha) okuyabilmektedir. Bunun için OCR sistemleri okunabilirliğini zorlaştırmak için gürültü değeri yüksek resim tabanlı Captcha oluşturulmuştur (Çakır ve Ulubatlı, 2018).

Kullanıcıya bir resim tabanlı bir test gösterilir ve kullanıcıdan bu uygun resimleri seçmesi isteniyor. Bu tür sistemlerin en büyük avantajı örüntü tanıma sistemleri için çözülmesi zor testler olmasıdır. Resim tabanlı Güvenlik kodları (Captcha) sadece resim içereceği gibi içine gömülü metinler de içermektedir. Resim karmaşıklığı, gürültüsü ve rotasyonu değiştirilerek OCR sistemlerin okumasını zorlaştırmaktadır. Binary resme dönüştürülen Güvenlik kodların (Captcha) karmaşıklığı ve gürültüsü oranında OCR sistemleri tarafından çözülmesi de o derece zorlaşmaktadır (Çakır ve Ulubatlı, 2018).

Ses tabanlı

Görsel tabanlı Güvenlik kodlarda (Captcha), kullanıcı testi tamamlamak için kendisine gösterilen karakterleri sisteme girmek zorundadır. Fakat makine öğrenmesinin gelişmesiyle birlikte bu tip uygulamaların çoğu botlar (kötücül yazılımlar) tarafından kırılabilir fakat buna rağmen bazıları bu tip ataklara karşı direnç göstermektedir. Resim tabanlı Güvenlik kodların (Captcha) en önemli dezavantajı düşünüldüğünde, ekran okuma programını kullanan görme yeteneği zayıf olan insanlar tarafından çözülememektedir. Bu bahsedilen tüm nedenlerden dolayı, görsel tabanlı Güvenlik kodlara (Captcha) alternatif olarak ses tabanlı Güvenlik kodlar (Captcha) geliştirilmiştir. İki sistem türü resim ve ses tabanlı Güvenlik kodlar (Captcha) genellikle aynı ara yüzde bir arada oluşturulmaktadır. Ses tabanlı Güvenlik kodlarda (Captcha), kullanıcı bozulmuş değişime uğramış bir ses mesajını dinleyip daha sonra duyduğu sesi tanımak ve istenen karakterleri (harf veya rakam) sisteme girmek zorundadır. Bu tip uygulamalarda genellikle, zararlı yazılımlara karşı sistemi güçlendirmek için, sesin normal yapısının bozulması için bazı ses bozma teknikleri de kullanılmaktadır (Çakır ve Ulubatlı, 2018).

Ses tabanlı uygulamalar, görsel tabanlı uygulamalardan daha zordur. Bu tip uygulamaların en büyük dezavantajlarından biri kullanıcının idrak kabiliyetini strese uğratabilir ve rahatsız edebilir. Kullanıcının sistemi geçebilmesi için, rastgele şekilde kendisine yöneltilen bir grup rakam veya karakteri hafızasında tutması gerekmektedir. Bu da kullanıcının kısa süreli hafızasını zorlamasına sebep olmaktadır. Hatta ses mesajında aşırı derece ses bozma teknikleri kullanıldığında, kullanıcıların %50'sinden fazlası en popüler ses tabanlı Güvenlik kodları (Captcha) başarıyla geçememektedir. Genel olarak ses tabanlı Güvenlik kodları (Captcha) iki ana kategoriye ayrılabilir. Birinci kategoride ses mesajına birçok deforme edilmiş rakamlar veya karakterler kullanılmak suretiyle arka plan sesi eklenerek kullanıcıya sunulmuş olanlar, ikinci kategoride ise kullanıcıya bir ses mesajı ile birlikte ilişkili bir resim sunulmaktadır (Çakır ve Ulubatlı, 2018).

2.2.2. İki katmanlı

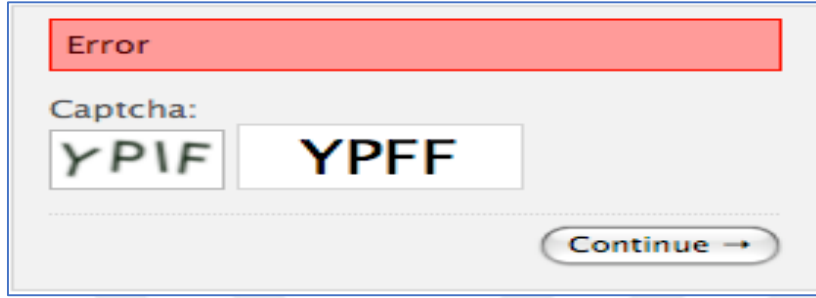
İki katmanlı Güvenlik kodları (Captcha) metin tabanlı, görüntü tabanlı ve ses tabanlı Güvenlik kodları (Captcha) kullanılarak ikili kombinasyonların oluşturulmasıdır. Resim tabanlı Güvenlik kodlarına (Captcha) metin karakterlerin gömülmesi ya da ses tabanlı Güvenlik kodlarına (Captcha) metin karakteri yazdırma gibi yapılar ikili Güvenlik kodlarına (Captcha) örnektir. İki katmanlı yapıda asıl amaç Optik karakter okuyucu (Optical Character Recognition-OCR) gibi sistemlerin Güvenlik kodlarını (Captcha) çözümlemelerini zorlamaktadır (Çakır ve Ulubatlı, 2018).

2.3. Captcha Gelişimi ve Türleri

Captcha uygulamalarının yayılmasıyla birlikte tersine Captcha uygulamalarının da siber suç işleyen gruplar tarafından geliştirilmiş ve böylece öngörülen sanal savaş başlamıştır. Bu grupların sürekli gelişen siber saldırılarına karşı koymak için yapılan Captcha uygulamaları daha karmaşık seviyelere ulaşmaktadır (Çakır ve Ulubatlı, 2018).

2.3.1. Basit captcha

Şekil 2.3.'de kullanılan Captcha çok basit ve gürültüsüz metin tabanlı ilk Captcha örneklerinden biridir. Bu tür Captchalar kötücül amaçlı uygulamalar tarafından çok özel şekilde hedef alındığında çok kolay aşılabilir (Github, 2013).



Şekil 2.3. Basit captcha (Github, 2013)

2.3.2. Güncel captcha

Basit Captcha aşılmaya başlanmasıyla, Captcha geliştiriciler Captcha yapılarını gürültülü, daha bulanık, eğri ve görüntüyü yabancı simgeler ve karalamalarla dolduran daha karmaşık çeşitler geliştirmeye başladılar.



Şekil 2.4. Güncel captcha (Ashamel, 2016)

2.3.3. Matematik captcha

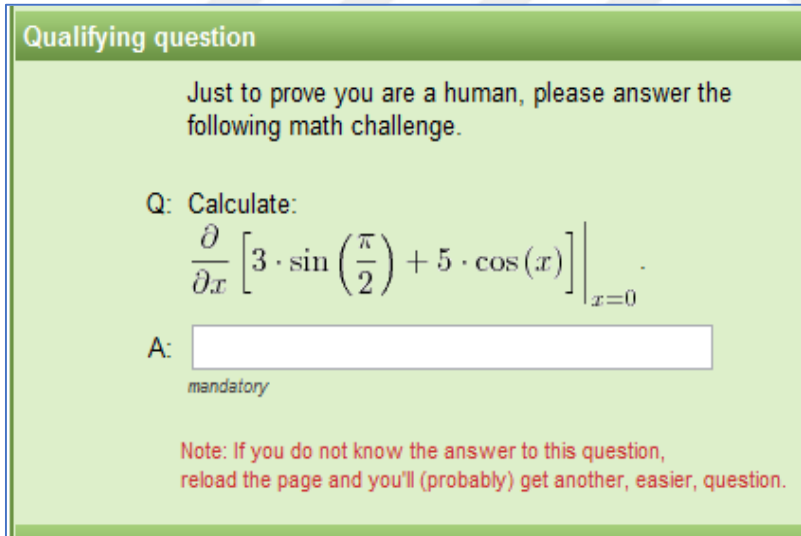
Basit matematiksel işlemlere dayanmaktadır. Şekil 2.5.'de $8+5$ gibi işlemlerin yapılması sonucun girilmesi istenmektedir. Amaçlanan geleneksel botların tümünü engellemektir. Fakat web sayfasına özel botlar engeli basitçe geçebilmektedir.



Şekil 2.5. Matematik captcha (Cluley, 2011)

2.3.4. Karmaşık captcha

Şekil 2.3.3.1'deki Captcha tasarımları her ne kadar güncel ve güvenli gözükse de farklı ve daha zorlu yaklaşımlara ihtiyaç olduğunu savunan ve çok daha karmaşık tasarımları kullanmayı tercih edenler de mevcuttur. Bu tasarıma en güzel örnek olarak Quantum Random Bit Generator (IRB, 2018) verilebilir. Quantum Random Bit Generator service üye olmak isteyenler Şekil 2.6.'daki karmaşık Captcha geçebilmek için karmaşık modeli çözmesi gerekmektedir (Çakır ve Uluhatun, 2018).

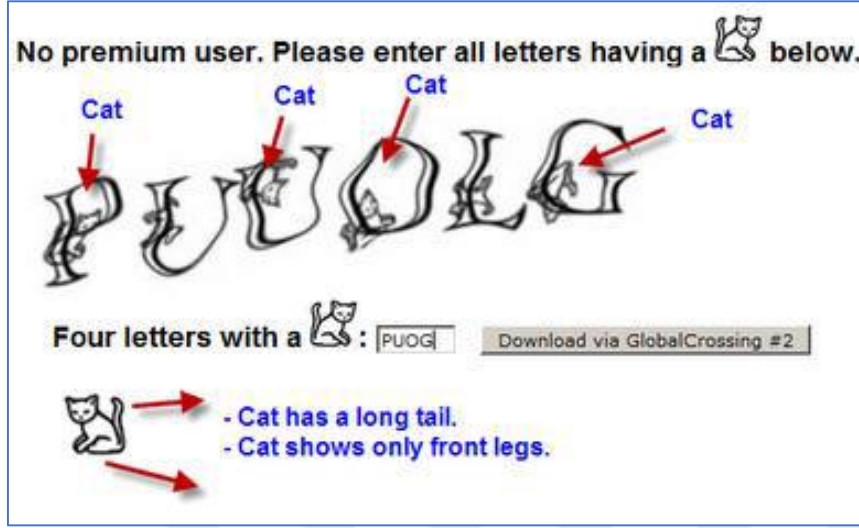


Şekil 2.6. Karmaşık captcha (Punk, 2008)

2.3.5. Nesneli captcha

Siber saldırılardan korunmak için sistemlerini korumaya alan tarafların bazıları zor Captcha uyarlamaları tercih ederken bazıları ise daha basit fakat yine de güvenlikten taviz vermeyeceği düşünülen daha farklı yöntemler kullanmaktadır. Şekil 2.7.'de görülen

uyarlama tarzında olduđu gibi klasik farklı açılarla eğriltilmiş harf ve rakam karakterlerinden başka işin içine resimlerin de katıldığı uygulamalar da mevcuttur.



Şekil 2.7. Nesneli captcha (Punk, 2008)

2.3.6. Resim captcha

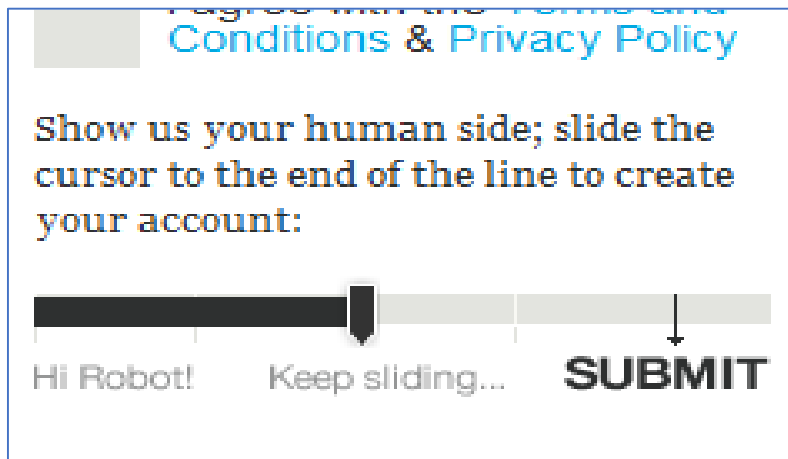
Captcha geçişi için kullanılan yapılarda anlamsız harf/rakam kombinasyonları kullanma sınırları kaldırıldıktan sonra nesneler Captcha uygulamalarında daha fazla kullanılmaya başlandı. İnternet hızlarının ve sunucu depolama kapasitelerinin artması ile çok daha güvenli ve can sıkıcı olmadığı düşünülen resim Captcha daha çok kullanılır olmuştur (Çakır ve Uluhatun, 2018).



Şekil 2.8. Resim captcha (Drupal Security Team, 2010)

2.3.7. Slider captcha

Uygulamaya giriş yapabilmek için sistemi ziyaret eden kullanıcılardan kaydırıcı sağa sürüklenmesi istenmektedir. Kaydırıcının gönder seçeneğine kadar getirilmesi durumunda gönderme butonu aktif olmaktadır böylece geçiş sağlanmış olur. Fakat özel ihtiyaçları olan insanlar için bu seviyede güvenliğin sağlanması zor olacaktır. Bu tarz uyarlamalar javascript ya da flash teknolojilerini kullandığı için kısıtlı ortamlarda kullanıldığında yedek bir doğrulama mekanizmasının olmasını gerektirmektedir (Çakır ve Ulubatun, 2018).

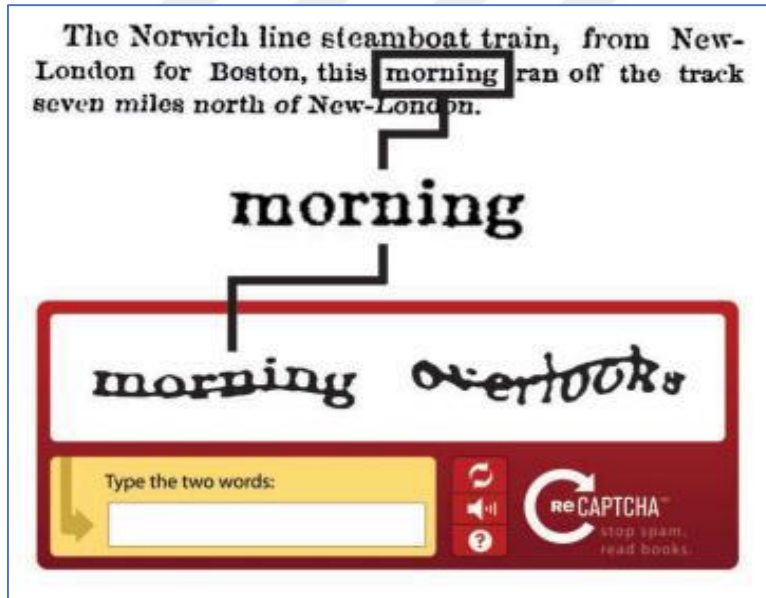


Şekil 2.9. Slider captcha

Şekil 2.9.'daki Captcha uyarlamaları ekranla etkileşime geçilmesi gereken uyarlamalar güvenli olmasına rağmen uygulama zorlukları sebebiyle pek tercih edilmemektedir.

2.3.8. ReCaptcha

Google Captcha servisini satın aldıktan sonra bu servise yeni fonksiyonlar katmıştır. Bu kapsamda; saldırganlar tarafından oluşturulan kötü niyetli otomatik yazılım botlarını engellemek için 2009 yılında reCaptcha'yı geliştirilmiştir. Eski kitap, gazete metnlerinin dijitalize edilmesinde kullanılmak üzere elde edilen OCR çıktıları kullanıcılar doğrulatacak şekilde reCaptcha olarak yeniden düzenledi. Doğrulama sırasında daha önceden başkaları tarafından doğrulanmış bir kelime ve ikinci bir tanımlanamamış kelime beliriyor; önceden tanımlanmış kelimeyi eşleştirerek insan ayırımı yapıldıktan sonra ikinci kelimeyi de Google Kütüphaneleri ve başka reCaptcha doğrulamaları için tanımlamış olmaktadır. (Bkz. Şekil 2.10.) Bu sayede Captcha uygulamalarının doğrulanması sırasında hem daha güvenilir sistem geçişi sağlanmıştır. Ayrıca Captcha metni okuma sırasında kaybedilen zaman, kullanıcılara kitap okutturmak gibi bir fayda sağlamaktadır (Luis, Maurer, McMillen, Abraham ve Blum, 2008; Çakır ve Ulubatun, 2018).



Şekil 2.10. ReCaptcha (Luis, Maurer, McMillen, Abraham ve Blum, 2008)

2.4. Captcha Genel Mantığı ve İşleyişi

Captcha uygulamalarında, doğrulama yapılabilmesi için üzerindeki yazıyı botların algılayamayacağı rastgele bir resmi sunucudan getirir ve kullanıcının bunu tanımlamasını ister. Kişi bu doğrulamayı yapana kadar sistemde ilerleyemez ve durum botlar için de farklı değildir. Buradaki temel ve önemli mantık, sunulan resmin sadece insanlar tarafından algılanabilecek yapıda olması ve botların tanımlayamayacağı şekilde oluşturulmasıdır (Çakır ve Ulubatlı, 2018).

Captcha resim yaratma adımları:

- Bitmap nesnesi yaratılır
- Bu bitmap nesnesinin yazı tipi, yazı biçimi gibi özellikleri düzenlenir.
- Bir rastgele nesnesi yaratılıp bu rastgele nesnesinin aralık değerleri yaratılır.
- Daha sonra rastgele bir değişken yaratılır.
- Bu rastgele dizgesi oturuma eklenir. Kıyaslamak için, kullanıcının girişi doğru yapıp yapmadığı test edilir.
- Son olarak isteğe bağlı olarak gürültü eklenir ve istenildiğinde karakter belirlenen bir açı ile döndürülür.

Önceleri basitçe yeterli olan bu uygulama tarzı, OCR (optical character recognition) adı verilen optik karakter tanımlayıcı programların gelişmesiyle ve programların giderek daha iyi sonuçlar vermesiyle artık resimler sadece insanlar tarafından tanımlanabilir olmaktan çıkmış ve yetersiz kalmıştır. Böylece Captcha gelişimi başlamıştır (Yan ve El Ahmad, 2007; Yan ve El Ahmad, 2008; Çakır ve Ulubatlı, 2018).

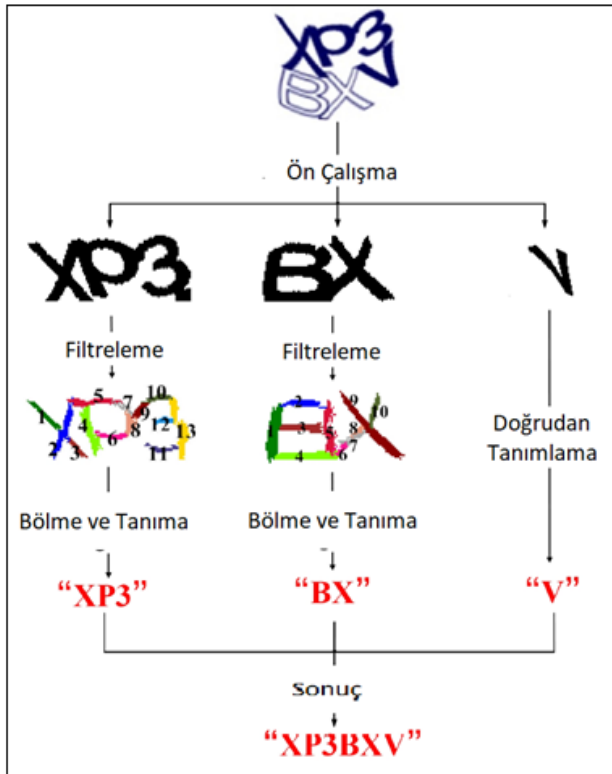
Karşıt uygulamalar ile yarışı sırasında Captcha her ne kadar değişik uygulama tarzları ortaya çıkmış olsa da temelde uygulamaların mantığı hep aynıdır. Bu mantık Turing testine dayanmaktadır.

2.5. DeCaptcha Adımları

Captcha her ne kadar zorlaştırılmış olursa olsun yine de kullanıcıların tanımlayabileceği zorluktadır, nitekim insanların dahi doğrulayamayacağı bir uygulama zaten amacının dışına çıkmış demektir. Kırılacak olan Captcha türü özelliklerine göre fazlara ayrılmalı ve

reCaptcha botu faz değiştirerek sonuca gitmelidir. En belirgin özellikleri ilk adımlarda eleterek ilerlemek en mantıklısı olacaktır (Çakır ve Ulubatun, 2018).

Örneğin klasik Captcha için arka fondaki parazitler ya da resmin üzerinden geçen düz çizgiler kurtarılabilecek ilk unsurlardır. Renk farkları ile renk seviyeleri değiştirilerek ve seviye aralıkları açılarak yazı fondan ayrılabilir. Şekil 2.11.' de kullanılan uyarlamalardaki gibi kirli fonlar, renk seviyeleri değiştirilerek kolaylıkla temizlenebilir. Yazının tamamen ya da karakter ve karakter eğikliğine karşı optik karakter tanımlama birkaç defa tekrarlanabilir. PWNtcha-Captcha Decoder (PretendWe're Not a Turing Computer but a Human Antagonist) uygulamasının amacı da birçok captcha modelinin verimsizliğinin ortaya koymaktır. PWNtcha bunu yapan birkaç uygulamadan sadece biridir (PWNtcha, 2017; Çakır ve Ulubatun, 2018).



Şekil 2.11. Captcha tanıma (Gao, Tang, Liu, 2017)

Karakterlerin arkasına belirsiz şekiller gömülmesi gibi daha karışık durumlarda ise siteye yönelik çok özel öğrenme ya da deneme, yanılma yöntemleri kullanan yapay sinir ağları kullanılmalıdır (Çakır ve Ulubatun, 2018; Ulubatun, Yalçın ve Alver, 2018).

Ses doğrulamaları yapılırken arka fon sesleri, gürültüleri insan sesi ve harf tanımlamalarına göre ayırt edilebilecek hale getirilerek bu uyarlamalar da aşılabılır hale getirebilir. Bu da yine yapay sinir ağı bilgi işlemleri aracılığıyla yapılabilecek bir işlemdir.

Captcha kırma temel algoritması

Karakter tanıma ve görüntü işleme

Captcha bitmap olarak aldıktan sonra bu bitmap dosyasını sayısal bir resme dönüştürür.

Sayısal resim

Bir resme ait en küçük noktaya piksel adı verilmektedir. 0 veya 1 değerini alırlar. Bu şekilde piksellerden oluşan resimlere ikili sayısal (binary) resim denilmektedir.

Renkli resimden gri resme dönüşme

Renkli olan bir resmi gri seviye resme dönüştürebilmek için orijinal resimdeki piksellerin her bir renk değerleri yerine, RGB renk modelinde bulunan gri-seviye renk değerlerine resmin özelliklerini değiştirmeden dönüştürülmesidir.

Threshold

Resmin belirli bir değerden daha büyük değere sahip piksellerin beyaz renge, daha küçük değere sahip piksellerin siyah renge boyanmasıdır. Captcha resimleri kullanırken threshold değeri genel de 128 alınır. Bu şekilde resim dizisini birler ve sıfırlardan oluşan siyah-beyaz bir diziye dönüştürülür.

Histogram çıkarma

Frekanslar grafikte gösterilerek histogramlar çıkartılır. Histogram, belli olan bir veri kümesindeki elemanların frekanslarıdır.

Karakterlerin ayrıştırılması

Her bir karakteri çevreleyen dikdörtgenin köşegenindeki koordinatlarının, yükseklik ve genişliğinin bulunmasıdır.

Genişletmek ve aşındırmak

Genişletmek bir resmi yapısal elemanla kesiştiği bölümler kadar büyütme. Sayısal bir resmin aşındırılmasıdır.

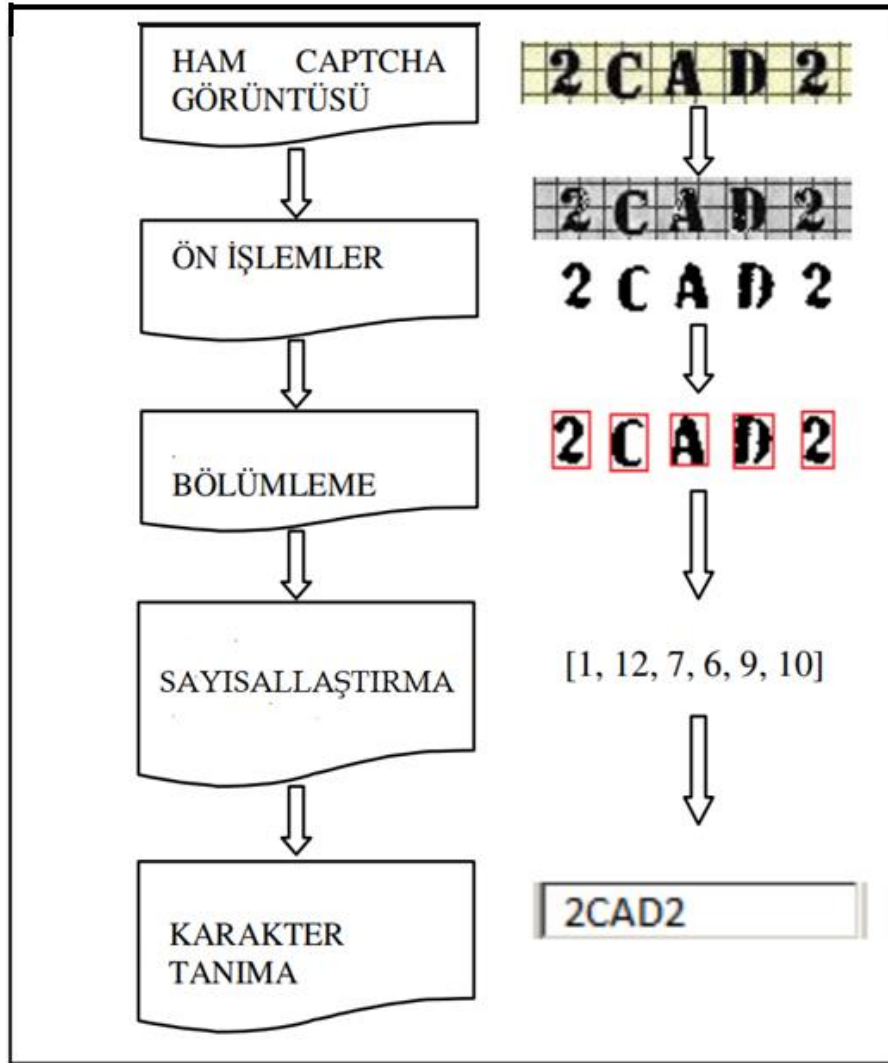
Filtreler

Görüntüdeki gürültüleri temizlemek için tanıma algoritmalarından önce median, mean ve gaussian filtreleri ile bu işlemi yapabilmektir.

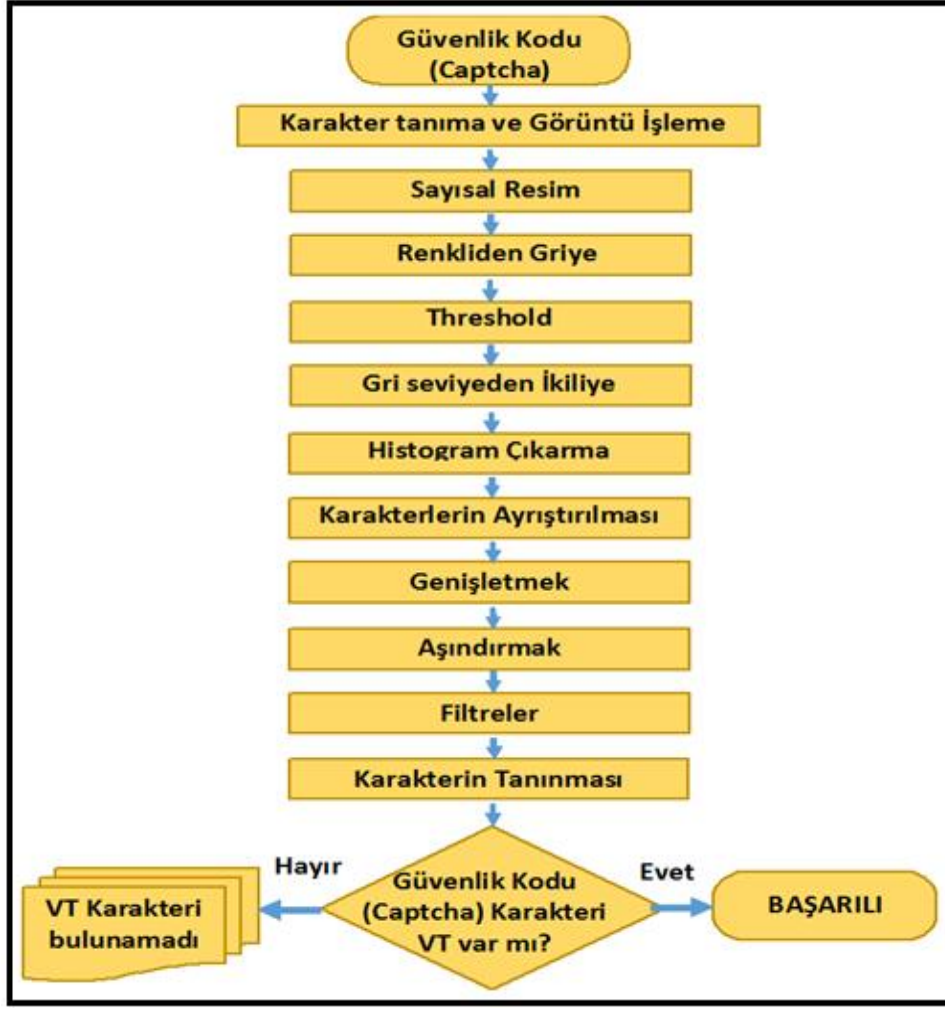
Karakterin tanınması

Karakter farklı görüntü işleme tekniklerinden geçtikten sonra histogramla ayrılarak belirlenmiş olan threshold değerine göre ikili (binary) diziyeye çevrilmesidir (Çakır ve Ulubatun, 2018; Ulubatun, Yalçın ve Alver, 2018).

Algoritmanın bu adımlarından sonra Captcha veri tabanı mevcut verilerle kıyaslandıktan sonra kod çözülmüş olur (Gao, Tang, Liu, 2017).



Şekil 2.12. Captcha kırma temel adımları (Eken, Sayar, 2015)



Şekil 2.13. Captcha kırma şeması

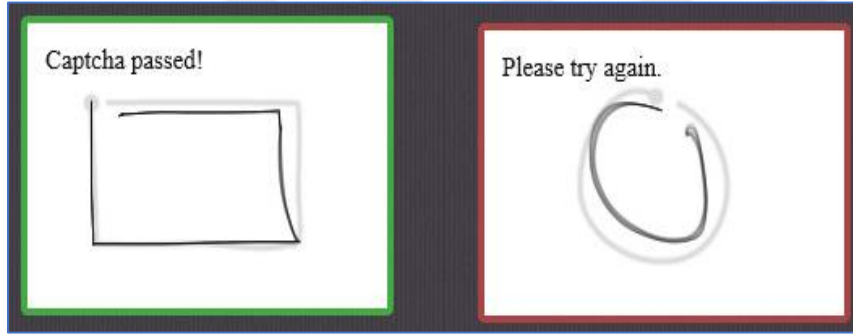
2.6. Captcha Yakın Geleceği

Captcha uygulamaları artık spamı engellemek isterken işlevselliğini kaybedip kullanıcıyı engelleyen ve canını sıkkan yapısından sıyrılıp ReCaptcha örneğindeki gibi daha modernize ve işlevsel duruma gelirken, bir amaç uğruna çalışır hale gelmiştir. Bu her ne kadar isteğe bağlı bir geliştirme gözükse de aslında mecburi bir harekettir. Günümüzde güvenli denilen uyarlamalar dahi yetersiz kalabilmekte ve geliştirilmesi gerekmektedir.

İnternetin devlerinden ve öncü firmalarından biri olan Yahoo bu konuya güzel bir örnek teşkil etmektedir. Yahoo Captcha sistemi %35'lik başarı oranıyla aşılmış (Kdawson, 2008) ve bu oran düşük gibi gözükse dahi çeşitli yollarla kötücül yazılım haline getirilmiş (botlaştırılmış) (Trojan/Truva, Virus, Worm) kitle bilgisayarları aracılığıyla etkili ve durmaksızın yapılan bir saldırıda hedef sistem için büyük tehlike arz etmektedir.

Kırılan sistemlerin ardından yapılan iyileştirme ve geliştirmeler aslında taraflar arasındaki savaşın çitasını bir kademe daha yükseltmektedir ve bu, sonuçta yazılım dünyasının, insanlığın kazancınadır. Resim Captcha ve sesli dinleyerek doğrulama olanağı geliştirmeleri bunun kanıtıdır; klasik uyarlamanın dışında olan ve işlevselliği arttırmaya çalışan bu iki yaklaşım da aşılarak daha sonrasında çitayı yeniden yükseltmiştir (Mims, 2011; Kleiner, 2008).

Bugünlerde yaygın olarak kullanılmasa da ileride video Captcha uygulamalarının benimseneceği ve gelişen dokunmatik ekran sistemleri ile resim Captcha gelişip el işareti, çizim doğrulamalarının ve uyarlamalarının (bkz. şekil 2.14. ve 2.15.) (Demirel ve Kılıç, 2011; Hall,2015; NuData,2017) revaçta olacağı aşikârdır. Hele ki günümüzde büyük öneme sahip olan Microsoft gibi bir yazılım devinin bile Captcha servisinin kırılmış olması bunun en büyük göstergesidir (Sharf,2012).



Şekil 2.14. Çizim captcha (Mims, 2011; Kleiner, 2008)



Şekil 2.15. Hareket captcha (Mims, 2011; Kleiner, 2008)

3D Captcha, insanın hayal gücü ve uzamsal perspektife dayanmaktadır. Temel fikir, özel bir 3D modelin dönüşümü ve doğru rotasyon pozisyonunun bulunmasıdır. Kullanıcının görevi,

doğru gözlem noktasını bulmak için modeli döndürmek ve captchayı başarıyla çözmektir (Çakır ve Uluhatun, 2018).

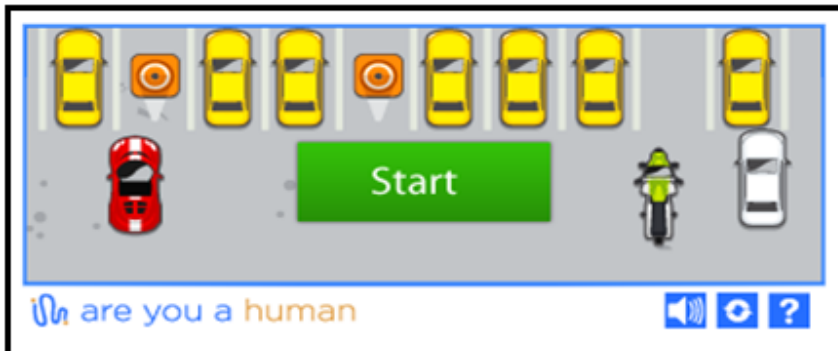


Şekil 2.16. 3D captcha (Mims, 2011; Kleiner, 2008)



Şekil 2.17. Key captcha (Mims, 2011; Kleiner, 2008)

Hoş ve keyifli bir Captcha oyunu ile ziyaretçileri eğlendirir. Resimdeki eksik parçaları tamamlanmasını sağlayan ufak bir bulmaca oyunudur.

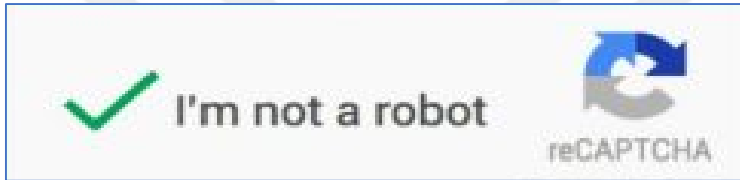


Şekil 2.18. PlayThru captcha (Mims, 2011; Kleiner, 2008)

PlayThru -HTML5 oyun tabanlı bir captcha, İnsan olduğunuzu ispatlamak için oyunu başarılı bir şekilde tamamlamanız gerekir. İngilizce'yi anlayan her insanın kolayca bitirmesi çok zor olmayan bir güvenlik kodudur (Çakır ve Uluhatun, 2018).

Google yeni captcha projesi

Google, uzun süredir kullanımda olan reCaptcha güvenlik adımının siteleri koruduğunu ancak oldukça hantal bir uygulama olduğunu belirtiyor. Bu düşünceyle ziyaretçilerin içeriklere ulaşma sürelerini hızlandırmak için yakın zamanda "*Ben robot değilim*" kutucuğunun tamamen gizli hale getirileceğini ve "*The Invisible reCaptcha*" duyurdu (Google,2017; Çakır ve Uluhatun, 2018).



Şekil 2.19. ReCaptcha (Google, 2017)

The invisible reCaptcha:

The Invisible reCaptcha amaçlanan; arka planda kullanıcıların IP adresini ve ekrandaki fare hareketleri gibi değişkenlerini takip edecek olan Google, sayfadaki kişinin insan mı yoksa bot mu olduğunu ayırt edebilecek. Böylelikle kullanıcılara "Sokak tabelası içeren kareleri seçin.", "Ağaç olan görselleri işaretleyin." ya da "Ekrandaki sayıları girin." gibi istekler yöneltilmeyecektir.

Makine öğrenimi (machine learning) ve gelişmiş risk analizinin (advanced risk analysis) bir birleşimi olan The Invisible reCaptchan'nın algoritma yapısı, güvenlik adımlarını çok daha hızlı gerçekleştirerek içeriklere anında ulaşılmasını sağlayacaktır (Çakır ve Uluhatun, 2018; Uluhatun, Yalçın ve Alver,2018).

Şekil 2.20. Invisible reCaptcha (Google, 2017)

2.7. Kullanım Alanları

Botlar (kötücül siber yazılımlar) kullanılarak çok çeşitli internet sitelerine zararlar verilebiliyor. Sistemlere bir insanın girebileceğinden çokça veri girerek verinin doğruluğuna zarar verilebileceği gibi yığın mesaj(spam) da yapılabilir (Çakır ve Ulubatun, 2018).

2.7.1. Web site üyeliklerini kontrol etmek

Web site üyeliklerinde genellikle yeni kayıt, kayıt unutma, kayıt yenileme işlemlerinde captcha kullanımı çokça tercih edilmektedir.

Yeni kayıt

Ağ (web) site üyeliğini kontrol etmek için üyelik ile sunulan ücretsiz hizmetlerden kötücül yazılımlar (botlar) kullanılarak milyonlarca üyeliğin alınması sağlanabiliyor. Sistemin bu şekilde milyonlarca elektronik mektup (e-mail) vs. hizmetler vererek çalışmaz hale gelmemesi için Captcha kullanılmaktadır (Çakır ve Ulubatun, 2018).

Şifreli giriş işlemi

Şifreli giriş ağ (web) sitelerinde giriş yapmak için Captcha kullanılmaktadır. Aksi durumda deneme yanılma yolu ile giriş test edilirken kullanıcı üyeliği kitlenir ya da sisteme giriş yapılmaya çalışılırken kullanıcı girişi bloke olmaktadır. Bu durum da kullanıcılar için

mağduriyet oluşturacaktır. Burada amaçlanan sisteme giriş yapmaya çalışmak ya da sisteme girişi engellemektir (Çakır ve Uluhatun, 2018).

Şifre unutmama

Şifreli giriş ağ (web) sitelerinde şifre unuttum kısımlarında şifre sahibini kontrol etmek için Captcha kullanılmaktadır. Kötücül siber yazılımın(botların) sisteme giriş başarılı olması durumunda şifre değiştir kısmında tekrar Captcha kullanılması güvenliği daha da sağlamlaştırır (Çakır ve Uluhatun, 2018).

Kritik işlem gerektiren durum

Şifreli giriş ağ (web) sitelerinde şifre unuttum kısımlarında, özellikle de ödeme sistemleri gibi kritik işlemlerin yapıldığı sayfalarda işlemi yapan insan mı yoksa kötücül yazılım (bot) mı ayrımı yapmak için Captcha kullanılmaktadır (Çakır ve Uluhatun, 2018). Böylelikle kritik işlem gerektiren ağ (web) sitelerinde sisteme giriş yapılmış dahi olsa Captcha ya da benzer ayrımı yapacak başka bir sistemin kurulması gerekmektedir.

2.7.2. Elektronik mektup adreslerini gizlemek

Yığın mesaj göndericiler (spammerlar), yığın mesaj (spam) yapabilmek için elektronik mektup (e-mail) adreslerini kullanıyorlar (Çakır ve Uluhatun, 2018). Bu elektronik mektup (e-mail)adreslerini bulabilmek için de ağda (web’de) metin (text) araması yapıyorlar. Bunu önlemek için de ağ (web) sayfalarında bir elektronik mektup (e-mail)adresini görebilmek için öncelikle Captchatestini geçmek ve işlemi yapanın insan olduğunu ispatlamak gerekmektedir.

2.7.3. Ağ günlüklerine yığın mesaj gönderilmesini önlemek

Çoğu ağ günlüğü (blog) yazarı yorum olarak gelen yığın mesajların (spam) farkındadırlar. Botların (kötücül yazılımlar) yazdıkları yığın mesaj (spam) şeklindeki yorumlar sayesinde arama motorlarında yığın mesajı (spam) yapılan web sitesinin üst sıralara çıkması amaçlanmaktadır. Bu durumun önüne geçebilmek için genellikle Captcha kullanılmaktadır (Çakır ve Uluhatun, 2018).Bu sayede ağ günlüğüne (blog) yorum yapmak için üye olmaya da gerek kalmıyor. Web site kullanıcının sadece ekranda gördüğünü yazıp, insan olduğunu kanıtlaması yeterli olması sağlanmaktadır.

2.7.4. Anketler

Anketler; Captcha gibi doğrulama sistemlerine en çok ihtiyaç duyan uygulamalardandır. Captchalar, botların herhangi bir anket seçeneğine birkaç dakikada milyonlarca oy vererek anket sonucun sağlıklı olmasını engeller.

2.7.5. Solucan virüs (worm) ve yığın mesajdan (spam) korunmak

Elektronik mektup(e-mail) yoluyla bulaşan virüslerden ve yığın mesajlardan (spam) korunmak istendiği zaman, “sadece insan tarafından yazılmış Elektronik mektup (e-mail) okumak istendiğinde Captcha tercih edilmektedir.

2.7.6. Arama motorları

Arama motorları kötüçül siber yazılımları (botları) genellikle kötüçül yazılım(bot) istemiyorum, indekslenmek (indexlenmek) istemiyorum etiketine (tag) saygı duyuyorlar. Genellikle bu durum daha çok büyük arama motoruna sahip şirketler için geçerli. Diğer arama motorlarına sahip şirketlerin genellikle başvurdıkları yol ise; giriş sayfasına konulan bir güvenlik kodudur (captcha) (Çakır ve Ulubatun, 2018).

2.8. Güvenliği Sağlamadaki Rolü

Temelde Güvenlik Kodu (captcha, completely automated public turing test to tell computers and humans apart) ana amacı, bilgisayarlar ve insanlar arasındaki ayrımı yapmak üzere tasarlanmış bir güvenlik mekanizmasıdır. Ve kötü niyetli programlara (bot) karşı korunma amaçlı kullanılır.

Bölüm 2.7.’de belirtilen kullanım alanlarında ve daha birçok yerde Captcha güvenliği sağlamada kullanılmaktadır. 2.7.1. web site üyeliklerinde kullanılmasındaki amaç sisteme gerçek kullanıcının giriş yapmasını sağlamaktır. Bölüm 2.7.2. elektronik mektup (e-mail) adreslerini gizlemek için kullanılmasındaki asıl amaç; Elektronik mektup(e-mail) adreslerini ele geçirilmesinin ve kötüçül amaçlar için kullanılmasını engellemektir. 2.7.3. ağ günlüklerine (blog) yığın mesaj (spam) gönderilmesini önlemedeki asıl amaç; arama motorlarında iyi ya da kötü ün getirecek şekilde üst sıralarda çıkmasını sağlamaktır. Bölüm 2.7.4. anketlerde kullanılmasının asıl amacı; anketi yapılan konu hakkında sağlıklı gerçek sonuçlar ortaya çıkmasını sağlamaktır (Çakır ve Ulubatun, 2018). Bölüm 2.7.5. worm ve

spam korunmak için kullanılır böylelikle sadece insan tarafından yazılmış e-mailler gelen kutusunda görülür. Bölüm 2.7.6. arama motorlarında Captcha kullanılmasının nedeni; arama motorlarında, web sitelerin üst sıralarda çıkmasına neden olan indekslenmeye engel olmaktadır.





3. LİTERATÜR DEĞERLENDİRİLMESİ

Captcha ve Turing Test kullanımı ile ilgili literatür araştırmaların sonucu aşağıda kısaca özetlenmiştir.

Gazi Bilişim Enstitüsü Adli Bilişim Bölümünden (Çakır ve Uluhatun, 2018)'nın yaptıkları çalışmada, Güvenlik kod (captcha) türleri ve yapılan Güvenlik kod (captcha) çalışmaları baz alınarak daha güvenli bir Güvenlik kod (captcha) kombinasyon testi sunulmuştur. Önerdikleri yaklaşım temelde üç aşamadan oluşmaktadır. İlk aşamada kullanıcının Güvenlik kod (captcha) ile imtihanını zorlaştırmamak için metin tabanlı basit Güvenlik kod (captcha) ile test edilmesi istenmiştir. İkinci aşamada, ilk aşama testi başarısız olduğunda metin ve resim tabanlı daha zorlaştırılmış Güvenlik kod (captcha) testi sunulmuştur. Üçüncü aşamada ise ilk iki aşamadan daha karmaşık ve kullanıcıyı zorlayacak farklı tabanlı Captcha sunulmuştur. Bu yaklaşım ile kullanıcı ile bot ayırımı daha kolay yapılabilmiş ve oluşturulan Captcha birleşim çeşitliliği ile bot programlarının algoritmasına meydan okunabilir olduğu gösterilmiştir.

(Abdala, 2017) Captcha üzerine yaptığı çalışmada, saldırıları azaltmak için web güvenliği alanında captcha stratejisinin kullanılmasına odaklanmıştır. Bulmacalara dayanan metinler de dahil olmak üzere, farklı metin, resim, ses ve video tabanlı Güvenlik Kodları (Captcha) araştırılmıştır. Türk üniversitelerinin öğrencilerin özel bilgi sayfalarını korumak için kullandıkları Captcha çeşidine ışık tutmuştur. Metin ve resimden oluşan Captcha tipi inceledikten sonra kırılmış ve tanınmıştır. Kırma ve tanıma süreci için bir Mozilla eklentisi kullanılmış ve Java programı oluşturulmuş. OCR tekniği kullanılarak, Metin ve resimden oluşan Captcha tipinin zayıflığı kanıtlanmıştır. Yapılan çalışmayla kullanılan 53 tane metin ve resim Captcha örneğinden %92,45'inin kırılabilir ve tanınabilir olduğu gösterilmiştir.

Bir diğer çalışmayı da Atılım Üniversitesi Fen Bilimleri Enstitüsünden (Elatresh, 2019) yapmıştır. Libyalı öğrencilerin WWW ortamında farklı Captcha tiplerine yönelik tutumlarını belirlemesi amaçlamıştır. Araştırmanın amacına ulaşmak için bir anket hazırlanmış ve farklı düzeylerde ve bölümlerde okuyan Libyalı öğrenciler internetten yayınlanan ankete cevap verilmiştir. Elde edilen veriler SPSS 18.0 yazılım paketi kullanılarak işlenmiştir. Sonuçlar, katılımcıların sürekli Web'de kitap ya da bilimsel makaleler bulmak için gezindikleri için Captcha türlerine aşina olduklarını gösterilmiştir. Ancak, metin tabanlı Captcha için kullanıcı aşinalığı diğerlerinden daha yüksek olduğu tespit edilmiştir. Captcha türü olan

reCaptcha, hatalara karşı duyarlılık, kolaylık ve güvenlik dahil olmak üzere farklı bakış açılarından en çok öne çıkan olduğu tespit edilmiştir.

(Gao, Tang, Liu, 2017) yapılan çalışmada; 2015 yılında Microsoft'un oluşturduğu iki katmanlı yeni Captcha şeması incelenmiştir. Bu iki katmanlı şema ilk olması bakımından önem taşımaktaydı. Bu nedenle, oluşturulan bu iki katmanlı Captcha, tasarımcılarının beklediği kadar güvenli mi? Sorusuna cevap aranmıştır. Bunun için yaptıkları çalışmada iki katmanlı Captcha'nın güvenliğini sistematik olarak ilk kez analiz etmişlerdir. Microsoft tarafından uygulanan iki katmanlı Captcha'ya saldırmak için basit ama etkili bir yöntem önermişler ve saniyede ortalama hız 9,05 standart bir masaüstü bilgisayarında %44,6 (3,3 GHz Intel Core i3 CPU ve 2GB RAM ile) başarı oranı elde etmişlerdir, bu durum güvenlik açığı sorununu ortaya koymuştur. Saldırı sonucunda 2015 yılında Microsoft'un yapmış olduğu iki katmanlı Captcha modeli kırılmıştır. Saldırıların özgünlüğünü ve uygulanabilirliğini tartışılmıştır ve daha iyi bir güvenlik ve kullanılabilirlik ile Captcha tasarlamak için yöntemler sunmuşlardır.

Newcastle Üniversitesi'nden (Tayara, 2017) tarafından yapılan çalışmada; Captchaların özellikle metin tabanlı olanların kırılabilirliklerini ortaya konmuştur. Ve bu sebeple Captchalara hareket eklemek için yeni bir yaklaşım ortaya koymuştur. Bu amaçla 3 soruya cevap aranmıştır. İlk soru: Yeni Captcha programlarına dahil edilen canlandırma teknikleri, saldırılara karşı gereken sağlamlık seviyesini sağlayabilir mi? İnceleme sonucu, canlandırılmış özellikleri kullanan Captcha programlarının çoğunun kırılabileceğini göstermiştir. İkinci soru: En son standart metin tabanlı Captcha şemalarında kullanılan segmentasyon direnci mekanizması, animasyon şemalarında kaçırılmayan saldırılara karşı gerekli ilave direnç seviyesini sağlayabilir mi? reCaptcha ve Wikipedia Captchanın son sürümüne karşı yaptığı test, onlara yönelik yüksek başarı oranı sağlayan yeni saldırı mekanizmalarına karşı güvenlik açığı sorunlarına neden olduğunu göstermiştir. Üçüncü soru: Güvenlik ve kullanılabilirlik arasında iyi bir denge sağlayabilecek animasyonlu metin tabanlı bir Captcha programı tasarlamak için ne kadar alan vardır? Standart ve animasyonlu metin tabanlı Captcha yaptığı saldırıların sonuçlarına dayanarak; tasarladığı yönergeleri kullanarak yeni bir animasyonlu metin tabanlı Captcha tasarlamış ve daha sonra bu soruyu cevaplamak için güvenliğini ve kullanılabilirliğini test etmiştir. Saldırıların ayrıca, daha önce de belirtildiği gibi, güvenlik ve kullanılabilirlik açısından tasarlayıp test ettiği izleme ve bölümlendirme saldırılarına direnç sağlayabilecek animasyonlu metin tabanlı Captchalar için bir kılavuz sağlamıştır. Araştırma ayrıca mevcut Captcha tasarımında daha dayanıklı bir

planının nasıl tasarlanacağını daha iyi anlaşılmasını sağlamak için Captcha kullanılabilecek sağlamlık ve kullanılabilirlik konularının bir listesine ek olarak Captcha kırılması için bir araç kutusu oluşturulmasına da katkıda bulunmuştur (Tayara, 2017).

King Abdulaziz Üniversitesi Bilgisayar Bilimleri Fakültesinden (Alharbi, 2016) tarafından yapılan çalışmada; tüm kullanıcılar için yüksek kullanılabilirliğe sahip yüksek erişilebilirliğe sahip bir Captcha geliştirmeyi ve aralarında bir ilişki modeli olan hem görüntü hem de sesi olan yeni bir Captcha oluşturmayı hedeflemiştir. Sistem, saldırganın kaynaklara istenmeyen erişime izinsiz girmesini engellerken insan kullanıcısının istenen web sitesine erişmesine izin vermelidir. Her kullanıcı, yetenekleri ve yeteneklerinden bağımsız olarak, web veri içeriğine çok kolay ve asgari engellerle erişme hakkını hak ederken, bilgisayarların ve robotların çözmesini imkansız kılıyorsa, iyi bir Captcha sistemi olduğunu gösterir. Güvenli bir bot önleme tasarımıyla, muazzam bir erişilebilirliğe ulaşma hedefini gerçekleştirmek için gerçekleştirdiği dost canlısı Captcha sistemini sunmuştur. Böylece, metin ve görüntüye dayanan mevcut Captchalara, dost canlısı Captcha'nu oluşturmak, test etmek ve karşılaştırmak için araştırma çalışmaları yapılmıştır. Dost canlısı Captcha'nun metodolojisini belirlemek ve Captcha sisteminin erişilebilirliğini arttırmada kolaylığını kanıtlamak için nihai sonuçları değerlendirilmiştir.

West Wirgina Üniversitesi West Virgina Üniversitesi Bilgisayar Bilimleri ve Elektronik Mühendisliği Bölümü öğrencilerin (Powell, 2018) tarafından yapılan çalışmada; mevcut uygulamaların eksikliklerini gideren Captcha'ların tasarımını önermiştir. Bu Captcha'lar kullanıcıların yüz tarama, yüz tanıma, multimodal biyometrik tanıma ve insan olduklarını kanıtlamak için nesne tanıma dahil, farklı görüntü tabanlı görevler gerçekleştirmelerini gerektirir. Bunlar, insanların başarılı oldukları ancak bilgisayarların başarılı bir şekilde tamamlanması için zor olan görevlerdir. Ayrıca, geleneksel bilgisayarlarda ve mobil cihazlarda kullanımlarını kolaylaştıran, tıklama veya dokunma tabanlı giriş yöntemleri kullanılarak kolayca gerçekleştirilebilirler. Bu çalışmada geliştirilen Captcha'lar, insan başarısı yüksek oranlarını mümkün kılmak ve ihmal edilebilir otomatik saldırı başarı oranlarını sağlamak için çeşitli stratejiler kullanmıştır. FgCaptcha tarafından kullanılan bu tür bir teknik, üretilen her bir Captcha görüntüsünün çözülmesinde sırasıyla insan kullanıcılarının ve otomatik saldırganların simülasyon performansını temsil eden bir tness değerini hesaplamak için, görüntü kalitesi ölçümlerini ve yüz algılama algoritmalarını kullanmıştır. Genetik bir öğrenme algoritması, her Captcha görüntüsü için özelleştirilmiş üretim parametrelerini belirlemek için bu belirsizlik değerlerini kullanmıştır. Bu

araştırmada, üretilen Captcha görüntülerini optimize etmek için, gradyan iniş öğrenme, yapay bağışıklık sistemleri ve çok aşamalı performans dayalı öğrenme süreçleri gibi diğer yaklaşımlar da önerilmiştir. Bu araştırmada geliştirilen Captcha'ların test edilmesini ve analizini kolaylaştırmak için kapsamlı bir RESTful web servis tabanlı değerlendirme platformu geliştirilmiştir. Kullanıcılar, çeşitli aygıtlar kullanarak bu Captcha'ları çözme konusunda 180.000'den fazla girişimde bulunmuşlardır. Sonuçlar, bu araştırmada yaratılan tasarımları insan başarı oranlarının yüksek olduğunu göstermiştir.

Delaware Üniversitesi Bilgisayar Bilimleri ve Elektronik Mühendisliği Bölümü öğrencisi (Greene, 2018) tarafından yapılan çalışmada; kaç tane web sayfasının captcha sistemi kullandığını bulmak için en iyi 30.000 Alexa web sayfasını taranmıştır. Diğer hedefini ise, captcha türlerini sınıflandırmak ve herhangi bir zayıf yan veya zayıflığa sahip olup olmadıklarını belirlemek için bilinen Captcha'ları değerlendirmiştir. Giriş, at arabası, abone ol, parola, imza, kaydol, katıl gibi anahtar kelimeler arayarak, en iyi 30.000 web sayfasını ve web sayfalarının URL'sindeki captcha'ların ayrıştırılması için Beautiful Soup kütüphanesini kullanan bir web tarayıcısı tasarlamıştır. Auth, upload, hesap ve kayıt gibi ilk 30.000 web sayfasını taradıktan sonra, web sayfalarının yalnızca 10.017'sinin captcha sistemleri kullandığını göstermiştir. Bulduğu captcha'lar ses tabanlı, görüntü tabanlı, metin tabanlı, captcha, reCaptcha, FunCaptcha, kaydırıcı, matematik, özel ve metin / görüntü tabanlı captchalar olduğunu göstermiştir.

(Hart, 2019) yaptığı çalışmada; reCaptcha, doğru uygulandığında, talep edenin bir robot değil bir insan olduğunu kanıtlayarak çeşitli otomasyon saldırılarını önlemeye çalışır. ReCaptcha çözümleri genellikle bu araştırmanın anlamaya çalıştığı çeşitli yöntemlerle atlanabilmiştir. Bu araştırmanın amacı, reCaptcha çözümlerinin uygulama düzeyinde atlanmasına neden olabilecek olası sorunları gözden geçirmek olduğunu belirtmiştir. Bu araştırmanın yol açtığı sorular, reCaptcha bypasslarına ilişkin hangi güvenlik açıklarının mevcut olduğunu, yanlış bir güvenlik duygusu yaratan reCaptcha uygulamalarının nasıl olduğu ve reCaptcha kullanan uygulamaların güvenliğini artırmak için neler yapılabileceğini içermiştir. Bu araştırma, reCaptcha bypasslarının çoğunda, geliştiricilerin reCaptcha'nın nasıl uygulanacağını doğru şekilde anlamadıkları sonucu olarak ortaya çıktığını tespit edildiği gibi Google ve yüksek rütbeli arama sonuçları da dahil olmak üzere çok sayıda uygunsuz reCaptcha kurulum kılavuzunun bulunduğu ortaya konmuştur. Bu araştırma, tahmin edilebilecek en muhtemel sekiz reCaptcha bypass yönteminin yanı sıra, bir güvenlik test cihazı olarak saldırganın nasıl test edileceği tanımlanmıştır. Yanlış uygulanan bir

reCaptcha çözümü nihayetinde otomasyon saldırılarına karşı koruma sağlamaz. Araştırma bulguları tarafından belirlenen tavsiyeler Google'ın oldukça makul bir şekilde uygulayabilmesi için, geliştiricilerin reCaptcha uygulamalarının atlanabileceğini göstermek için otomatikleştirilebilir korumalar getirmiştir.

Troy Üniversitesi Bilgisayar Bilimleri Bölümünden (Ramya, 2015) tarafından yapılan çalışmada; çoğu güvenlik ilkeleri zorunlu ve zorlu matematik problemleri üzerine geliştirilmiştir. Güvenlik için zorlu bir Yapay Zeka (AI) sorunu henüz tamamen keşfedilmemiş ilginç bir yeni paradigmadır. Bu tezde, Yapay Zeka sorunlarına dayanan yeni bir güvenlik protokolü gösterilmiştir. Grafiksel şifreler olarak Captcha (CaRP), yani, Captcha teknolojisi üzerine inşa edilmiş grafiksel şifre sistemlerinin bir kombinasyonu tanıtılmıştır. Grafiksel şifreler olarak Captcha, hem bir grafiksel şifre şeması hem de Captcha teknolojisinin bir kombinasyonunu içerir. Her şey düşünüldüğünde, röle saldırılarıyla birlikte çevrimiçi tahmin saldırıları (online guessing attacks together with relay attacks) ve omuz sörfü saldırıları (shoulder-surfing attacks) gibi bir dizi güvenlik sorununu da ele almıştır. Genel olarak, bir CaRP şifresi, şifrenin düzenli olarak aranmasına rağmen otomatik olarak çevrimiçi tahmin saldırılarıyla mümkün olabilir. Ayrıca, görüntü sıcak nokta sorununu (the image hotspot problem) tanımak için yenilikçi bir yaklaşım sunar. Popüler grafiksel parola sistemlerinden biri olan ve genellikle zayıf parola kararlarına yol açan geçiş noktaları, tamamen olmada da l, makul güvenlik ve kullanılabilirlik sunmuştur. Çevrimiçi güvenlik sorunlarını gidermek için bazı pratik uygulamalara layık ve uygun görünmüştür.

Yapılan bir diğer inceleme çalışması da; görsel ve sesli Captcha'lardaki güçlü ve zayıf yönleri tartışmaktır. Görsel Captcha'ların parçalanmasındaki temel teknikler detaylı bir şekilde tartışılmıştır. Kullanılabilirlik özellikleriyle ilgili hususlar, kullanıcılara anket yoluyla ulaşılarak, kullanıcı ilgisinin seçilmesiyle incelenmiştir. Metin tabanlı Captcha'lardaki risklerden kaçınmak için rastgele görüntüler insan görünüm özelliklerine bağlı olarak üretilmiştir. Görme engelli kullanıcılar bu tür Captcha'lara yaklaşamadıkları için, mevcut kaynaklara yaklaşımlarını önledikleri için yine bu sınırlıdır. Teknoloji geliştikçe profesyonel programcılar ses Captcha'larını da kırmanın yollarını bulunmuşlardır. Bu güvenlik açıklarından korunma önerileri de kısaca tartışılmıştır (Saikirthig ve Vaithyasubramanian, 2016).

Captcha üzerine yapılan çalışmalardan biri de; captcha internet güvenliğinde önemli bir rol oynar ve bir araya getirme karakter segmentasyonu hala captcha tanıma araştırmasının bir sorundur. Bu çalışmada, dikey projeksiyona dayanan bir captcha segmentasyon yöntemi,

captcha tanıma doğruluğunu arttırmak için hem sayı hem de harfleri birleştiren Captcha'daki farklı tiplerdeki konglutasyon karakterlerinin segmentasyon problemini etkili bir şekilde çözebilmiştir. Öncelikle, engelleme arka planını kaldırma, ses çıkarma ve ikili hale getirme, daha az gürültülü ikili captcha görüntüsü alma dahil olmak üzere captcha görüntüsüne ön işleme tabi tutulmuştur. İkinci olarak, captcha karakter segmentasyonuna geliştirilmiş dikey projeksiyon yöntemini uygulanmıştır, farklı kümelenmiş tip karakterlere hedeflenen segmentasyon yöntemini önerilmiş ve tek karakterli görüntü elde edilmiştir. Üçüncüsü, tanıma için şablon eşleştirme algoritmasını kullanarak örnek ve şablon karakter piksellerinin örtüşme hızını eşleştirme oranı olarak alınmıştır. Son olarak, yukarıda açıklanan segmentasyon ve tanıma algoritmalarına ulaşmak için program deneyi ile sonuçlandırmıştır. Deneysel sonuç, bu makalede önerilen yöntemin konglütinat karakterler üzerinde etkili segmentasyon etkisine sahip olduğunu ve dolayısıyla captcha tanımanın doğruluğunu arttırdığını göstermiştir (Zhang, Xie, Luan ve He, 2017).

Yapılan çalışmalardan biri de captcha; açık web kaynaklarını otomatik erişime karşı korumak için yaygın olarak kullanılan bir araştırma alanıdır. Captchanın amacı, otomatik yaklaşımları en aza indirerek her kullanıcıya orijinal hizmetler sunmaktır. Verimli bir Captcha sadece insan dostu değil, aynı zamanda Captcha testini geçmek için yapılan makine saldırılarına dayanacak kadar sağlam olmalıdır. Literatürde metin tabanlı, video tabanlı, matematiksel veya soru bazlı gibi birçok Captcha önerilmiştir. Kötücül yazılımlar, optik tanıma veya makine öğrenim teknikleri kullanarak bu Captcha testini etkin bir şekilde atlamaya çalışmışlardır. Captchanın tasarımı ve uygulanması yapay zeka alanında dayanmaktadır. Modern dijital dünya tarafından etkin bir şekilde kullanılacak ve optik tanıma ve diğer otomatik saldırıların azaltılmasına yönelik bir Captcha tasarlama amaçlanmıştır. Bu çalışmada, daha iyi güvenlik sorunları için, sayısal mantık kapıları kullanarak Matematiksel Boole cebirine dayanan dijital Captcha adı verilen OCR olmayan bir Captcha tasarımı önerilmiştir. Farklı mantık kapıları (AND, OR, NOT, NAND, NOR) gibi şekilleri gösteren tasarımıdır. Her kapı, Boole yasalarını kullanarak Boole cebirine dayanarak birden fazla yanıt yürütür. Kullanıcı kanıtlamak için, kullanıcı mantık kapılarının şekillerini tanıyabilir ve birden fazla cevaptan doğru bir cevap seçer. Deneysel sonuçlar, farklı yaş gruplarına sahip birden fazla teknik ve teknik olmayan kullanıcı tarafından analiz edilmiştir. Ortaya çıkan değerler, önerilen sistemimizin yüksek olasılık ve güvenlik düzeyine sahip olduğunu ve mevcut matematik Captchalarıyla yapılan görsel saldırılara karşı koyduğunu göstermiştir (Kaur, 2016).

Arizona Üniversitesi Bilgisayar Bilimleri Bölümünden (Gutierrez, 2017) tarafından yapılan çalışmada; toplam 282 çevrimiçi web uygulamasından veri toplanmıştır. Ve kimlik doğrulama uygulamaları, çok aşamalı kimlik doğrulama uygulamaları, güvenlik sorusu uygulamaları, geri dönüş kimlik doğrulama uygulamaları ve çevrimiçi hesaplar için diğer güvenlik uygulamaları hakkında veri toplamak için bu web uygulamalarının 230'unun hesapları oluşturulmuştur. Çevrimiçi hesaplar için şifre gücü analiz edildi ve parola gücü verileri mevcut verilerle karşılaştırılmıştır. Çevrimiçi hesaplar tarafından kullanılan güvenlik soruları, güvenlik ve kullanılabilirlik açısından değerlendirilmiş ve geri dönüş kimlik doğrulama uygulamaları, en iyi uygulamalara bağlılıklarına göre değerlendirilmiştir. Alternatif kimlik doğrulama şemaları incelenmiş ve HTTPS ve Captcha'ların kullanımı gibi diğer güvenlik hususları araştırılmıştır. Mevcut verilere dayanarak, parola politikaları, 2017'deki web uygulamalarında 2010'daki gereksinimlere göre daha güçlü parolalar gerektirdiği gösterilmiştir. İncelenen çevrimiçi web uygulamalarının yaklaşık dörtte birinde güvenlik soruları kullanılıyor ve bu soruların çoğunun kullanılabilirlik ve güvenlik endişelerin varlığı tespit edilmiştir. HTTPS ve sürekli kimlik doğrulama gibi güvenlik mekanizmaları genel olarak çoğu web uygulaması için güvenlik sorularıyla birlikte kullanılmaz ve bu da web uygulamasının genel güvenliğini azaltır. Web uygulamalarının çoğu, giriş bilgisi ve şifre kurtarma bilgisi olarak e-posta adreslerini kullanır ve en iyi uygulamaları izlemez. Yaklaşık dörtte biri çok aşamalı kimlik doğrulamayı kullanır ve dörtte biri sürekli kullanılır kimlik doğrulaması, ancak çoğu hesap savunma için güvenlik önlemlerini derinlemesine birleştirmek için başarısız olduğu belirtilmiştir. Genel sonuç, bazı çevrimiçi web uygulamalarının güvenli uygulamalar kullandığı; ancak, çevrimiçi web uygulamalarının çoğu, güvenli uygulamaları doğru şekilde uygulayamıyor ve kullanamıyor olduğu gösterilmiştir.

Hong Kong Çin Üniversitesi Bilgisayar Bilimleri Bölümünden (Ching, 2016) tarafından yapılan çalışmada; bir çerçeve geliştirilmesi ile başlanmıştır. Birleşik birleşik matris faktörleşmesine dayanarak kalabalık kaynak sistemlerinde dinamik koşullar altında çalışanlara görev önerilmiştir. Çerçeve bir faktör analizi modelinden oluşan ve öğrenen bir algoritmasıdır. Oluşturulan çerçeve sadece çalışanların görev seçimindeki tercihlerini değil aynı zamanda performans tarihçelerini de dikkate almıştır İşçi derecelendirmelerini etkileşimli davranışlarından çıkarıyor ve bu dönüşüm, kitle kaynaklı sistemlerde görev önerisine etkin bir şekilde yardımcı olmuştur. Karmaşıklık analizi, çerçevenin verimli olduğunu ve büyük veri kümelerine ölçeklenebilir olduğunu göstermiştir. Gerçek dünyadaki

veri kümeleriyle yapılan deneylere dayanarak, sonuçlar, çerçevenin en gelişmiş teknolojiye uygun bir şekilde daha iyi performans gösterdiğini göstermiştir. Bu tezde, oluşturulmuş olan çerçevedeki çalışanlara kalite güvencesi için kitle kaynaklı sistemlerde görev önermek amacıyla aktif bir öğrenme algoritması önerilmiştir. Aktif öğrenme algoritması çok düşük maliyetle kesin doğruluk sağlayabilmiştir. Deneysel sonuçlar algoritmanın, çerçevenin performansını artırabileceğini göstermiştir.

San Diego Eyalet Üniversitesi Bilgisayar Bilimleri Bölümünden (Thakur, 2017) tarafından yapılan çalışmada; internette web sitesi güvenliği ve kullanıcı gizliliği bugünlerde büyük endişe kaynağı olmuştur. Gündelik hayatımızda internet üzerinden yüzlerce web sitesinde sörf yapıyoruz. Ziyaret ettiğimiz her web sitesi, kullanıcı adı ve kullanıcı adı vererek giriş yapmalıdır. Bu geleneksel giriş kimliği ve parola düzeninin dezavantajları sunulmuştur; Bunların ilki, arkamızda veya yanımızda duran bir kişi, biz yazarken şifreyi kasıtlı olarak görebilir. (Shoulder-Surfing). İkincisi, birisi klavye (Keylogger) yazılımını bilgisayarımıza yüklediye, şifremiz başkalarına açıklar. Bu tezin amacı, yukarıda belirtilen sorunların üstesinden gelebilecek ve web üzerindeki güvenliği artıracak bir uygulama oluşturmuştur. Akıllı Giriş (Smart Login), gelecekte bu tür bir güvenliğin web üzerinden uygulanabileceğini gösteren bağımsız bir uygulamadır. Bu uygulama kullanıcıların şifrelerini doğrudan girmelerini sağlamaz, dolaylı olarak da kimliğini doğrular. Bir kullanıcının giriş ekranında sadece giriş kimliğini girmesi gerekir. Her oturumda yeni bir oturum şifresi üretilir, böylece orijinal şifrenin arka uçta sağlam tutulması, sistemin daha güvenli olmasını sağlamıştır.

James Madison Üniversitesi Müzik Sanatları Bölümü (Yampiro, 2016) tarafından yapılan çalışmada; Robert Paterson'ın Captcha'sı, yorumlayıcı bir bakış açısıyla bazı benzersiz zorluklarla gelen bariton ve piyano için beş şarkıdan oluşan bir döngüdür. Metin, Captcha'lardan oluşur: orijinal olarak bir bilgisayarın kimliğine karşı insan kimliğini test etmek için tasarlanmış iki kelimelik ifadelerdir. Hemen hemen her cümle anlamsız bir kelime ve gerçek bir kelime içerir ve uygun bir sözdizimi yoktur. Bu çalışmada, bir "doğru" cevap yazmadan, olasılıkların çeşitliliğini keşfetmek için multidisipliner bir yaklaşım izlemiştir. Bir literatür taraması, konser vokalleri, şarkı sözleri için sıradan metinler kullanan diğer şarkılar, gerçek ve saçma sözcükleri birleştiren üç özel metin ve Lewis Carroll, Nuvoletta, James Carroll tarafından hazırlanan "Jabberwocky" de dahil olmak üzere, Captcha'ya paralellikler çizen çeşitli türleri araştırılmıştır. Çalışma çeşitli bulguları sentezler ve müziğin ve metnin karakterinin keşif için bir temel oluşturabileceği yorumlama için

stratejiler üretmiştir. Çalışma, basit bir metin içermeyen bir eserin ve daha fazla araştırma yapılacak alanların incelenmesinin yararları hakkında kısa bir özetle sonuçlanmıştır.

(Robertson, 2018) tarafından yapılan çalışmada; mevcut akademik araştırmaların, hükümet politikalarının ve popüler medyanın araştırılması, AI (Yapay Zeka) siber saldırılarının teorikten pratik bir yapıya hızla dönüştüğünü ve daha fazla farkındalık, acil müdahale ve daha fazlasını gerektiren meşru bir tehdit faaliyeti ortaya koyduğunu ortaya koymuştur. Bu çalışma yapay zeka ile geliştirilen sosyal mühendislik saldırılarını, kendi kendini düzelten kötü amaçlı yazılım üreten makine öğrenme uygulamalarını ve diğer AI (Yapay Zeka) algoritmalarını gerçek dünyaya zarar verme potansiyeli ile bozan AI saldırılarını analiz ederek AI (Yapay Zeka) siber saldırılarındaki eğilimleri sunmuştur. Bulguların tartışılması, insani bileşeni siber saldırılardan tamamen ortadan kaldırma potansiyeline sahip AI'nın özerk sistemlere evrimini ve ABD federal hükümetinin bu meseleleri yakın akran rakiplerine karşı uluslararası ölçekte nasıl ele almaya çalıştığını içermiştir. Daha ileri araştırma önerileri, AI'nın bütünlüğünü ve açıklanmasının yanı sıra AI (Yapay Zeka) tabanlı bir silahlanma yarışı olasılığını ve mevcut özerk yapay zekanın yasal ve etik zorluklarını sağlayan teknik çözümleri keşfetme fırsatı sunmuştur.

Huazhong Bilim ve Teknoloji Üniversitesi Bilgisayar Bilimleri Bölümünden (Wan, 2016) tarafından yapılan çalışmada; sunucuların içeriğini gizlice ve ısrarla tarayan tarayıcıları tespit etmek ve sınırlamak için PathMarker adlı yeni bir tarayıcıyla mücadele mekanizması geliştirilmiştir. Temel fikir, her web sayfası URL'sine bir işaretleyici eklemek ve ardından URL'yi ve işaretleyiciyi şifrelemektir. İşaretleyicide bulunan URL yolunu ve kullanıcı bilgilerini algılama modüllerimizin yeni özellikleri olarak kullanarak, en erken dağıtılan tarayıcıların çoğu bile gizli tarayıcıları doğru bir şekilde saptayabilmiştir. Tarayıcıları etkili bir şekilde tespit etmenin yanı sıra, PathMarker, aynı sayfanın URL'sini ziyaret eden tarayıcıları farklı işaretçilerle yanıltmak suretiyle tarayıcıların verimliliğini de önemli ölçüde bastırabilmiştir. Yaklaşımımızı normal kullanıcıların verilerini toplamak için bir forum web sitesinde kullanılmıştır. Değerlendirme sonuçları, PathMarker'ın 12 açık kaynaklı ve şirket içi tarayıcının yanı sıra iki harici tarayıcıyı da (yani Googlebots ve Yahoo Slurp) hızlı bir şekilde yakalayabildiğini göstermiştir.

Yapılan bir diğer çalışmada; internet, e-posta ve arama motorları gibi birçok web servisinin mevcudiyeti ile günlük hayatımızda giderek daha önemli bir rol oynamaktadır. Ancak, bunlar genellikle botlar gibi bilgisayar programlarının saldırılarıyla tehdit altındadır. Bu sorunu ele almak için, bilgisayar programları ve insan kullanıcıları arasında ayırım yapmak

için Captcha geliştirilmiştir. Bu mekanizma iyi güvenlik sağlaması ve web servislerine otomatik kaydı kısıtlansa da, bazı korsanların Captcha mekanizmasına sızmasına izin veren bazı zayıflıkları vardır. Bu çalışma çeşitli CAPTCHA yöntemleri ve kategorileri ile ilgili son araştırmaları incelemiş, bu tür zayıflık ve gücü tartışılmıştır (Khalifa ve Hasan, 2016).

Literatür taraması; incelenen ulusal, uluslararası doktora tezi, yüksek lisan tezi ve makaleler sonucunda ele edilen bilgilerin konu olarak özetlenmiş hali Şekil 3.1., Şekil 3.2. ve Şekil 3.3.'de gösterilmektedir.

ÇALIŞMA TÜRÜ	ÇALIŞMA KONUSU	KAYNAK
Makale	Captcha çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması: Hata sayısına göre zorlaşan kullanıcı dostu captcha model kombinasyon tavsiyesi	Çakır, H. ve Uluhatun, (2018). <i>Güvenlik Kodu Çeşitliliği ile Siber Tehditlere Karşı Güçlü güvenliğin sağlanması</i> , International of Human Sciences Journal ISSN:2458-9489 Volume 15 Issue 3
Makale	İki katmanlı Microsoft Captcha kırılabilir olduğunu gösteren bir çalışma	Gao, H., Tang, M., Liu, Y., Zhang, P. ve Liu, X. (2017), <i>Research on the Security of Microsoft's Two-layer Captcha</i> IEEE Transactions on Information Forensics and Security, IEEE Transactions on Information Forensics and Security (Volume: 12, Issue: 7, July 2017)
Makale	Kriptografi ve yapay zeka ile farklı captcha modelleri geliştirmek	Von Ahn, L., Blum, M., Hopper, N. J. and Langford, J., <i>Captcha: Using hard at problems for security</i> , in Advances in Cryptology/EUROCRYPT 2003. Springer, 2003, pp. 294-311.
Makale	Yahoo mail üzerinden Captcha işleyiş mantığı: Turing Test	Von Ahn, L. , Blum, M. . Hopper, N. J and Langford, J. <i>Telling humans and computers apart automatically</i> , Communications of the ACM, vol. 47, no. 2, pp. 56-60, 2004.
Makale	Metin tabanlı captchaların güçlü ve zayıf yönlerin belirlenmesi ve tavsiyeler	Bursztein, E., Martin, M. and Mitchell, J. <i>Text-based captcha strengths and weaknesses</i> , in Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011, pp. 125-138.
Makale	Captchaların kullanılabilirliği veya Captcha tasarımıyla kullanılabilirlik sorunları	Yan, J. and Ahmad, El A. S. <i>Usability of captchas or usability issues in captcha design</i> , in Proceedings of the 4th symposium on Usable privacy and security. ACM, 2008, pp. 44-52.
Makale	Bölümleme tabanlı insan dostu HIP (Human Interaction Proof, Captcha)'ler oluşturmak	Chellapilla, K., Larson, K., Simard, P. Y. and Czerwinski, M. <i>Building segmentation based human-friendly human interaction proofs (hips)</i> , in Human Interactive Proofs. Springer, 2005, pp. 1-26.
Makale	Tek karakter tanıma ile bilgisayarların HIP (Human Interaction Proof, Captcha)'leri yenmesi	C. Kumar, L. Kevin, S. Patrice, Y., and C. Mary, <i>Computers beat humans at single character recognition in reading based human interaction proofs (hips)</i> , in CEAS 2005- Second Conference on Email and Anti-Spam, July 21-22, 2005, Stanford University, California, USA, 2005.

Şekil 3.1. Literatür taraması(a)

Makale	Naif örüntü tanıma algoritmalarıyla görsel Captcha 'ları kırmak	Yan, J. and El Ahmad, A. S. <i>Breaking visual captchas with naive pattern recognition algorithms</i> , in <i>Computer Security Applications, Conference, 2007. ACSAC 2007. Twenty-Third Annual. IEEE</i> , 2007, pp. 279–291.
Makale	Microsoft Captcha'ya düşük maliyetli saldırı	Yan, J. and El Ahmad, A. S. <i>A low-cost attack on a Microsoft captcha</i> , in <i>Proceedings of the 15th ACM conference on Computer and communications security. ACM</i> , 2008, pp. 543–554.
Makale	Tablo arama programının Turing testini geçebileceği iddiası üzerine bir çalışma	McDermott, D. (2014), <i>On the Claim that a Look-Up Table Program could Pass the Turing Test</i> , <i>Minds and Machines</i> , 24: 143–88.
Makale	CAPTCHA: Güvenlik için güçlü AI sorunlarını kullanma	Ahn, L., Blum, M., Nicholas, J. H. and Langford, J. <i>CAPTCHA: Using Hard AI Problems For Security</i> Yorktown Heights NY 10598, USA
Doktora Tezi	Animasyonlu metin captchaların sağlamlığı,	Tayara, M. (2017). <i>Animasyonlu metin captchaların sağlamlığı</i> , Yayınlanmamış Doktora Tezi, Newcastle Üniversitesi Bilgisayar Bilimleri, İngiltere.
Doktora Tezi	Görüntü tabanlı Captchalar ile çevrimiçi güvenliğin artırılması	Powell, B.M. (2018). <i>Enhancing online security with image - based Captchas</i> , Yayınlanmamış Doktora Tezi, West Virginia Üniversitesi Bilgisayar Bilimleri ve Elektronik Mühendisliği Bölümü, ABD.
Doktora Tezi	Öğrenen algoritma ile kitle kaynaklı sistemlerde performansın artırılması	Ching M. (2016)., <i>Task recommendation in crowdsourcing systems</i> , Yayınlanmamış Doktora Tezi, Hong Kong Çin Üniversitesi Bilgisayar Mühendisliği Bölümü, Çin.
Doktora Tezi	Rastgele oluşturulmuş şarkı sözleriyle insan kimliğini oluşturma: Robert Paterson, captcha ve performansı hakkında kapsamlı sanatçının analizi	Yampiro K. D. (2016)., <i>Establishing human identity through randomly generated lyrics : a comprehensive performer's analysis of robert paterson's captcha and its performance</i> , Yayınlanmamış Doktora Tezi, James Madison Üniversitesi Müzik Sanatları Bölümü, ABD.
Yüksek Lisans Tezi	Kullanıcı dostu görüntü ve ses tabanlı güvenlik kodu incelenmesi	Alharbi, K. (2016). <i>Friendly security code - based image and audio</i> , Yayınlanmamış Yüksek Lisans Tezi, King Abdulaziz Üniversitesi Bilgisayar Bilimleri, Suudi Arabistan.

Şekil 3.2. Literatür taraması(b)

Yüksek Lisans Tezi	Türk üniversitelerinin öğrenci bilgilerini korumak için kullandıkları captcha sisteminin bir analizi	Abdala, K. H. (2017). <i>Türk üniversitelerinin öğrenci bilgilerini korumak için kullandıkları captcha sisteminin bir analizi</i> , Yayınlanmamış Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ
Yüksek Lisans Tezi	Üniversite öğrencilerinin CAPTCHA'ya yönelik tutumları	Elatresh, K. (2019)., <i>Üniversite öğrencilerinin CAPTCHA'ya yönelik tutumları</i> Yayınlanmamış Yüksek Lisans Tezi, Atılım Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
Yüksek Lisans Tezi	Geniş çaplı Captcha araştırması	Greene, M. (2018)., <i>Large scale Captcha survey</i> , Yayınlanmamış Yüksek Lisans Tezi, Delaware Üniversitesi Bilgisayar Bilimleri ve Elektronik Mühendisliği Bölümü, ABD.
Yüksek Lisans Tezi	Google uygulamasında uygulamaya dayalı baypaslar	Hart, C. (2019)., <i>Application based bypasses in Google implementation</i> , Yayınlanmamış Yüksek Lisans Tezi, Utica Enstitüsü, New York.
Makale	Bazı güçlü görsel Captcha'ların gelişimini ve zayıf ses Captcha'larını kırma	Saikirithig A. ve Vaithyasubramanian G., (2016)., <i>Review on development of some strong visual captchas and breaking of weak audio captcha</i> , International Conference On Information Communication And Embedded System(ICICES 2016)
Yüksek Lisans Tezi	Grafiksel şifreler olarak Captcha - zorlu AI problemlerine dayalı yeni bir güvenlik	Ranya, G. (2015)., <i>Captcha as graphical passwords-a new security primitive based on hard AI problems</i> , Yayınlanmamış Yüksek Lisans Tezi, Troy Üniversitesi Bilgisayar Bilimleri, Troy Alabama.
Makale	Web güvenliğini arttırmak için dijital kapıları kullanarak boole cebirine dayalı matematik captcha tasarımı için OCR dışı bir yaklaşım	Kaur R. (2016)., <i>A non ocr approach for math captcha design based on boolean algebra using digital gates to enhance web security</i> , This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference.
Makale	Gelişmiş dikey projeksiyona dayalı Captcha otomatik segmentasyon ve tanıma	Zhang L., Xie Y., Luan X. Ve He J. (2017)., <i>Captcha automatic segmentation and recognition based on improved vertical projection</i> , 2017 9th IEEE International Conference on Communication Software and Networks
Yüksek Lisans Tezi	Çevrimiçi güvenlik uygulamaları üzerine bir çalışma captcha kullanımı ve şifre dayanıklılığı tespit edilmesi	Gutierrez G. (2017)., <i>A study of online security practices</i> , Yayınlanmamış Yüksek Lisans Tezi, Arizona Devlet Üniversitesi Bilgisayar Bilimleri, Arizona.
Yüksek Lisans Tezi	Yapay zekanın siber saldırılardaki uygulamaları	Robertson W. A. (2018)., <i>Applications of artificuil intelligence in cyberattacks</i> , Yayınlanmamış Yüksek Lisans Tezi, Utica Enstitüsü Siber Güvenlik Bölümü, ABD.
Yüksek Lisans Tezi	Web içeriğini Kalıcı Tarayıcılara Karşı Koruma	Wan S. (2016)., <i>Protecting Web Contents against Persistent Crawlers</i> , Yayınlanmamış Yüksek Lisans Tezi, Huazhong Bilim ve Teknoloji Üniversitesi Bilgisayar Bilimleri, Çin
Yüksek Lisans Tezi	Captcha ile ilgili güncel bir araştırma	Khalifa W. ve Hasan A. (2016)., <i>A survey of current research on captcha</i> , International Journal of Computer Science & Engineering Survey (IJCSES) Vol.7, No.3, June 2016

Şekil 3.3. Literatür taraması(c)

Yapılan literatür taraması sonucunda incelenen tüm kaynakların özetlenmiş ve analizi yapılmıştır. Yapılan analizler sonucunda Captcha ile ilgili ilk çalışmaların 2003 ve 2004 yıllarında ortaya yeni yeni çıkmaya başladığı; 2016-2017 yılları ise Captchalarla ilgili en çok

alışmaların yapıldığı yıllar olduğu görölmektedir. Teknoloji gelişmesi ile birlikte siber dünyadaki gelişmeler sonucunda Captcha gibi doğrulama sistemlerine daha çok ihtiyaç duyulduğu ve ehemmiyet kazandığı sonucuna varılmıştır.

Şekil 3.1., Şekil 3.2. ve Şekil 3.3.'de gösterilen özet bilgilere göre Captcha ile ilgili yapılan çalışmaların çoğu ya captcha modellerini farklı yöntemlerle baypas edip kırmakla ilgili ya da yeni bir captcha modeli oluşturmaya dayanmaktadır. (Greene, 2018) çalışmasında Alexa verilerine göre en popüler web siteleri bir tarayıcı ile incelemiş ve captcha kullanım istatistiği çıkarmıştır fakat Google reCaptcha 2018 yılından itibaren gizli olduğu için tarama programları ile tespit edilmesi zordur ve bu çalışma sonucunun kesinliği konusunda soru işareti bırakmaktadır; (K. Elatresh, 2019) çalışmasında bir grup Libyalı öğrencilere internet üzerinden anket yolu ile captcha aşinalığı ve güvelliği test edilmiştir fakat bir grup baz alınarak ele alınmış olması istatistik sonucunu genellemeyi zorlaştırır; ve (Abdala, 2017) çalışmasında ise Türk üniversitelerin öğrenci bilgi sistemlerinde öğrenci bilgilerini korumak için kullandığı captcha çeşitlerini incelemiş ve %92,45'lik bir oran ile kırılabilir olduğu göstermiştir fakat bunu sadece üniversite siteleri incelemekle sınırlandırılmıştır. Literatür taraması ve özellikle bu üç çalışmadaki eksikler bu tezi oluşturmamı sağlamıştır. Türkiye'de en çok kullanılan web siteleri kullanım amacına göre gruplandırılarak captcha kullanım durumu incelenmiş ve böylece sitelerin eksik kalan yönleri belirlenip en güvenilir model sunulmaya ve siber saldırılara karşı önlem alınmasını sağlayıp farkındalık yaratacaktır.

4. YÖNTEM

Bu bölümde çalışma grubu, verilerin toplanması, verilerin çözümü ve yorumlanması, ve analizlerden elde edilen sonuçlara göre geliştirilen web sitesine yer verilerek; her bir alt başlıkla ilgili yapılan çalışmalar ayrıntılı bir şekilde açıklanmıştır.

4.1. Çalışma Kümeleri

Web tabanlı yazılımlar dışardan gelebilecek herhangi bir siber saldırıya karşı korunabilmek için bir takım güvenlik aşamalarından geçmektedir. Bu güvenlik aşamalarına katkıda bulunan yöntemlerden biri de Captcha kullanımıdır. Bu kapsamda; Alexa istatistik verilerinden ve arama motorlarında Türkiye’de en üst satırlarda çıkan 400 web sitesi uzman görüşleri de alınarak 340 siteye indirgenerek kullanım amaçlarına göre 16 grupta sınıflandırılmış, Çizelge 4.1 ve Çizelge 4.2.’de gösterilmiştir.

Çizelge 4.1. Captcha kullanım sayısı

İncelenen Captcha Sayısı	Captcha Kullanım Sayısı	Captcha Kullanmayan Sayısı
340	236	104

Çizelge 4.2. Web site kullanım amacı

Kullanım Amacı	İncelenen Site Sayısı
Arama Motorları	15
Sosyal Medya Siteleri	21
Haber Siteleri	30
E-Ticaret Siteleri	30
İlan Siteleri	10
Finansal Kurum Siteleri	30
Kişisel Siteler ve Bloglar	10
Eğitim Siteleri	55
Firma Siteleri	10
Sağlık Siteleri	42
Kamu Kurum Siteleri	15
Anket Siteleri	12
Eğlence Siteleri	30
Sanatsal Siteler	10
Portal Siteleri	10
E-Posta Servis Sağlayıcı Siteler	10
Toplam	340

İkincil ana grup olarak kullanılması en çok tercih edilen 8 çeşit Captcha bir grup haline getirilmiştir ve Çizelge 4.3.'de gösterilmiştir.

Çizelge 4.3. Kullanılan captchalar

Captcha Türleri	Kullanım Sayısı
Basit Captcha	39
Güncel Captcha	14
Matematik Captcha	24
Karmaşık Captcha	35
Nesneli Captcha	-
Resim Captcha	4
Slider Captcha	5
reCaptcha	111
reCaptcha + Matematik Captcha	1
reCaptcha + Karmaşık Captcha	1
reCaptcha + Resim Captcha	1
Matematik Captcha + Karmaşık Captcha	1
Toplam	236

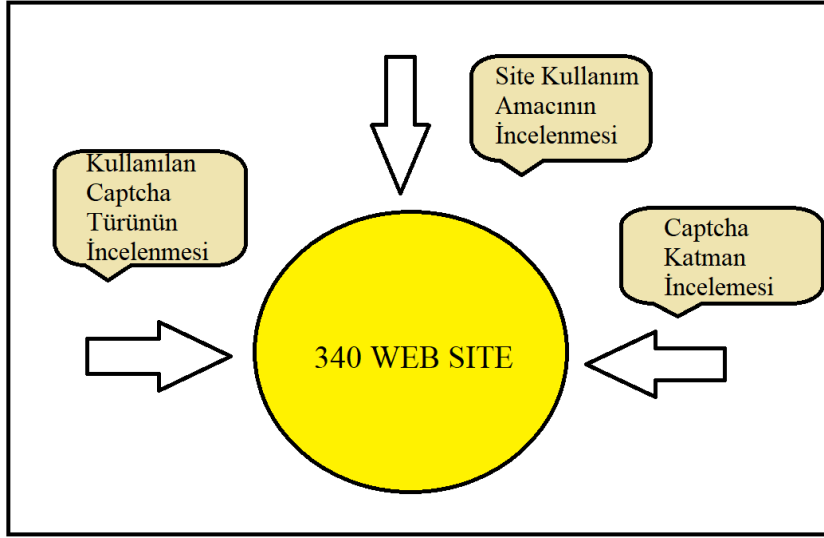
Captcha katmanları da üçüncül bir ana grup olarak ele alınmıştır. Bu grup da Çizelge 4.4.'de gösterilmektedir.

Çizelge 4.4. Kullanılan captcha katmanı

Captcha Katmanı
Metin Tabanlı
Resim Tabanlı
Ses Tabanlı

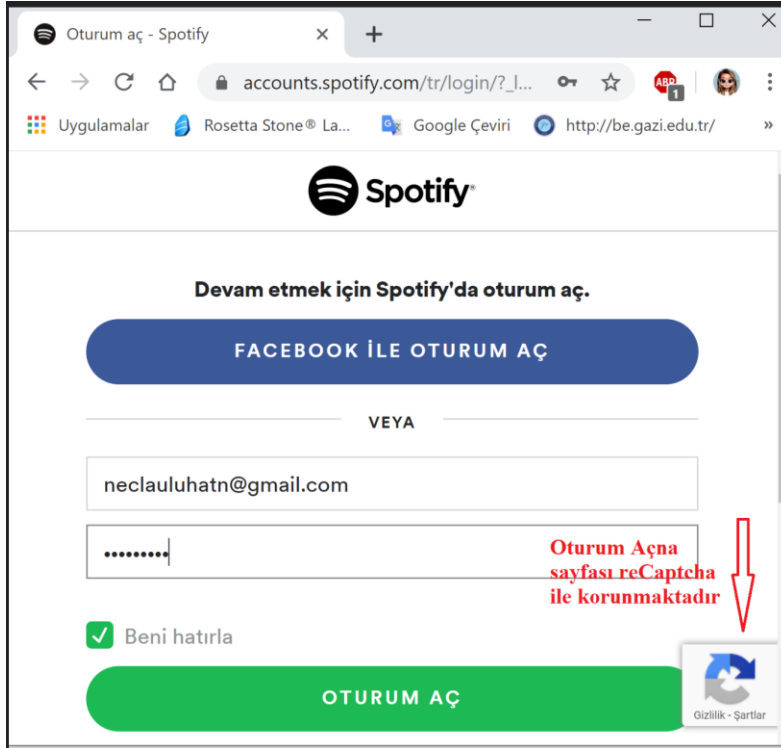
4.2. Verilerin Toplanması

Captcha kullanım oranları ve Captcha çeşitliliği web siteleri tarama yöntemiyle incelenmiş ve veriler toplanmıştır. Tarama yöntemi ile elde edilen veri kümesi, kullanım amaçlarına göre gruplandırılan web siteleri; Captcha kullanım durumlarına, kullanılan Captcha çeşitliliğine, Captcha kullanım amacına, kırılma oranına göre tek tek ele alınmış olup bu bulgularla ilgili sayısal veriler sunulmuştur.



Şekil 4.1. Verilerin toplanması

Veri toplama adımı taranacak web siteleri 16 amaca yönelik olarak sınırlandırılmış 340 web sitenin her birinde inceleme yapılırken; Captcha kullanımı mevcut mu? Eğer kullanıldıysa hangi tür katman ve çeşidi kullanılmıştır? Temel sorularına cevap aranarak veriler toplanmıştır.



Şekil 4.2. reCaptcha veri toplanması

En popüler müzik paylaşım platformu olan Spotify'dan veri toplarken, siteye giriş (account page) sayfasında sistemin reCaptcha ile korunduğu bilgisi hemen sayfanın alt tarafında Şekil 4.2.'de görülmektedir.

Öğrenci Bilgi Sistemi	
Öğrenci İçin Sistem Girişi	
Öğrenci no :	
Şifre :	[Unuttum!]
Bağlan	
Öğrenci kaydı bulunamadı...(Error 1002-1) Öğrenci no ve şifreyi kontrol ediniz...	

Şekil 4.3. Captchasız siteden veri toplanması

X Üniversitesinin öğrenci giriş sayfasını tarama yapıldığında herhangi bir Captcha modeli kullanılmadığı tespit edilmiştir. Şekil 4.3.'de görüldüğü gibi giriş sisteminde insan ve bot yazılım ayırımı yapacak bir yapı olmadığı için güvenlik açıklığına sahiptir. Bot uygulamaları ile X itesine yapılacak bir saldırı ile sisteme giriş mümkün kılınmıştır. X benzeri insan ve bot yazılım ayırımı yapmayan siteler arka planda bir güvenlik yöntemi kullanmak zorundadır. Bu yöntemlerden bazıları; cep telefona güvenlik kodu göndermek, e-mail ile doğrulama istemek, başka hesap ile bağlantı kurmak (e-devlet ile oturum açma, facebook ile oturum açma vb.), kısıtlı sayıda hatalı girişe izin vermek, kullanıcı hesabı kitleme ya da bloke etme, kullanım süresi sürekli takip edilmesi, tanımlanmayan kaynaklardan gelen girişleri engellemek vb. yöntemler sağlanabilir.

Şekil 4.4. Slider captcha veri toplanması-1

Şekil 4.5. Slider captcha veri toplanması-2

En popüler uluslararası e-ticaret sitelerinden biri olan Alibaba sitesi giriş sayfasında inceleme yapılırken Şekil 4.4. ve Şekil 4.5.'te görüldüğü gibi Slider Captcha kullanılmaktadır. Slider Captcha ile çift yönlü Turing test uygulanmış. Böylece bot saldırılarına daha çok meydan okuyabilmektedir denilebilir.

The screenshot shows the login page of Fikir SepetiM. At the top, there is a logo and the text "Hoşgeldiniz". Below this, a banner encourages users to complete surveys to earn Money points. The login form includes fields for "Money Club Kart No / Min No" and "Cep Telefon No". A red arrow points to the "Güvenlik Kodu" field, which contains a complex captcha made of numbers and letters. The captcha text is "xi02u". Below the captcha, there is a "Beni Hatırla" checkbox and a "Giriş" button.

Şekil 4.6. Karmaşık captcha veri toplanması

Türkiye’de en çok tercih edilen Migros market online alışveriş sitesinde inceleme yapılırken fikir sepeti sayfasında Şekil 4.6.’da Karmaşık Captcha kullanımı tercih edildiği görülmektedir. Böylece herkese açık olan bu sayfanın güvenliği arka planı gürültülü, rakam ve yazıdan oluşan karmaşık yapı tercih edilmiştir.

The screenshot shows the login page of İŞKUR (Türkiye İş Kurumu). The page title is "Şifre İşlemleri". The login form includes fields for "T.C. Kimlik No" and "Güvenlik". The "Güvenlik" field contains a mathematical captcha with the number "5684". Below the captcha, there is a "İleri" button and a red arrow pointing to the captcha with the text "Matematik Captcha Kullanılmış".

Şekil 4.7. Matematik captcha veri toplanması

Türkiye'nin önemli kamu kurumlarından biri olan İŞKUR web sitesinde inceleme yapılırken şifremi unuttum sayfasında Matematik captcha kullanımı Şekil 4.7.'de görüldüğü gibi tercih edilmiştir.

Şekil 4.8. Basit captcha veri toplanması

Türkiye Merkez Bankası web sitesinde inceleme yaparken şifremi unuttum sayfasında Basit captcha tercih edildiği Şekil 4.8.'de görülmektedir. Bunu tercih etme sebebinin arka planda daha güçlü güvenlik önemleri aldığı ve kullanıcıyı bunaltmak istemediği sonucu çıkarılabilir.

Şekil 4.9. Ses tabanlı captcha veri toplanması

Şekil 4.9.'da görüldüğü gibi Yandex sitesinde yapılan incelemede kullanıcı yenileme sayfasında basit captcha yanında ses tabanlı captchanın da kullanıldığı görülmektedir.

sahibinden.com

Üye Ol

☒ Bireysel Üyelik ☐ Kurumsal Üyelik ?

Adınız Soyadınız

E-Posta Adresiniz ?

Şifre Göster

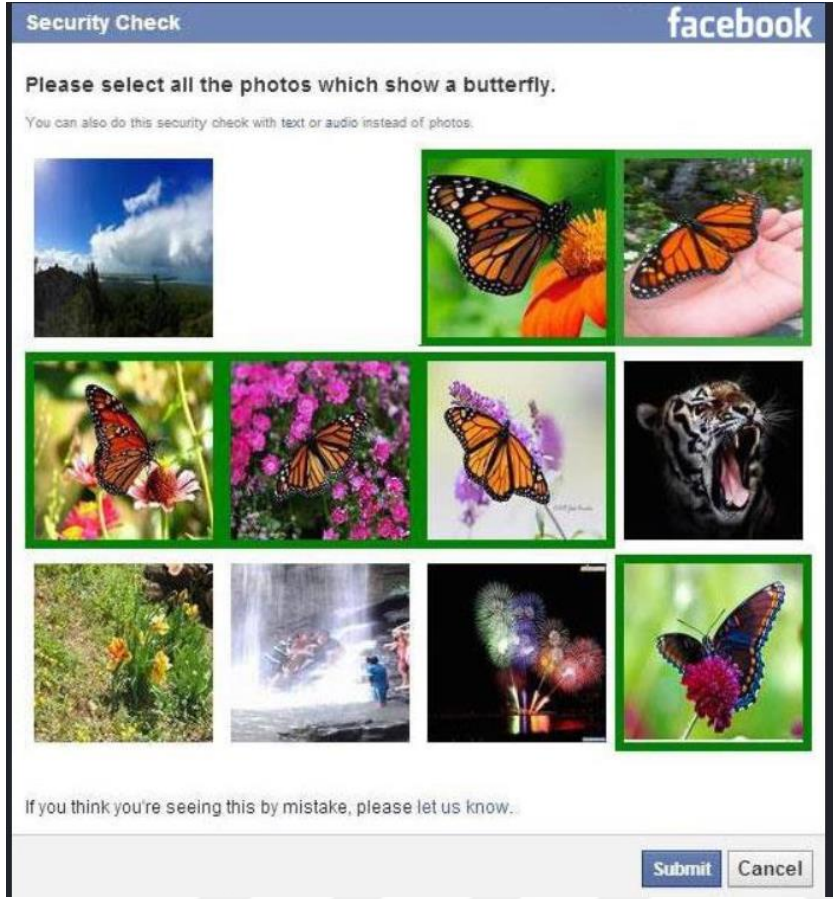
Güvenlik Kodu

kılıp

Arka plan resimli güncel captcha kullanılmış

Şekil 4.10. Güncel captcha veri toplanması

Şekil 4.10.'da görüldüğü gibi Sahibinde.com sitesinde yapılan incelemede üyelik sayfasında güncel captchanın kullanıldığı görülmektedir.



Şekil 4.11. Resim captcha veri toplanması

Şekil 4.11.'de görüldüğü gibi Facebook sitesinde yapılan incelemede özellikle hesap girişlerinde ya da hesap dondurma esnasında resim captcha sorularak işlemi yapan kişinin asıl kullanıcı olup olmadığı tespit edilmeye çalışılmaktadır.

4.3. Verilerin Çözümlemesi ve Yorumlanması

Araştırma ile ilgili elde edilen veriler yüzde frekans oluşturularak analiz edilmiş, daha sonra Bulgular ve Yorumlar bölümünde çizelgeler oluşturularak açıklanmış ve detaylı olarak yorumlanmıştır.

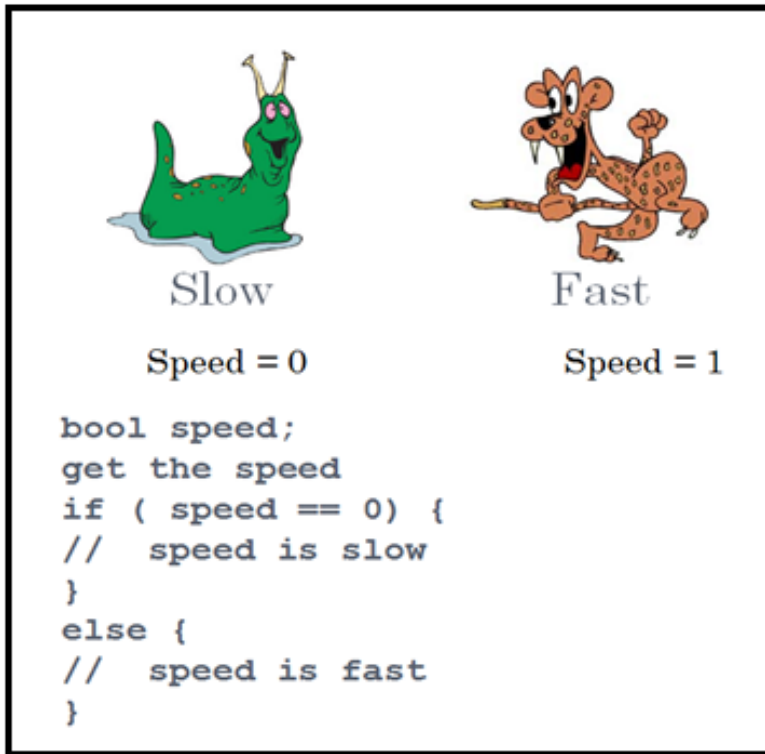
Çizelge 4.5. Özet çizelge

Kullanım Amacı	Basit Captcha	Güncel Captcha	Matematik Captcha	Karmaşık Captcha	Nesneli Captcha	Resim Captcha	Slider Captcha	reCaptcha	reCaptcha+ Matematik	reCaptcha+ Karmaşık	reCaptcha+ Resim	Matematik + Karmaşık
Arama Motorları	3	4	0	0	0	0	0	1	0	0	0	0
Sosyal Medya Site	0	3	0	0	0	4	0	12	0	0	0	0
Haber Siteleri	2	0	4	0	0	0	0	16	0	0	0	0
• Yerel	2		4					2				
• Ulusal	0		0					5				
• Uluslararası	0		0					9				
E-Ticaret Siteleri	0	3	0	1	0	0	3	8	0	0	0	0
• B2B		1		0			1	3				
• B2C		1		1			1	0				
• C2C		1		0			1	5				
İlan Siteleri	2	0	0	2	0	0	0	3	0	1	0	0
Finansal Kurum Site	4	1	0	6	0	0	1	10	0	0	0	0
• Banka	3	1		5			0	1				
• Borsa	1	0		1			0	2				
• Kripto Para	0	0		0			1	7				
Kişisel Siteler ve Bloglar	1	0	1	0	0	0	0	2	0	0	0	0
Eğitim Siteleri	6	0	6	10	0	0	0	11	0	0	0	1
• Okul	3		1	2				3				1
• Üniversite	2		0	1				7				0
• Dershane	0		3	0				0				0
• Uzaktan Eğ.	1		2	2				1				0
• Yayınevi	0		0	5				0				0
Firma Siteleri	2	0	0	4	0	0	0	4	0	0	0	0
Sağlık Siteleri	9	0	5	7	0	0	0	7	1	0	0	1
• E-Randevu	1		2	1				1	0			0
• E-Tahlil	2		2	0				3	0			0
• Hastane	1		0	3				2	1			1
• Eczane	5		1	3				1	0			0
Kamu Kurum Siteleri	2	0	5	1	0	0	0	6	0	0	0	0
Anket Siteleri	1	0	0	0	0	0	0	9	0	0	1	0
Eğlence Siteleri	6	0	1	1	0	0	0	7	0	0	0	0
• Oyun	3		0	0				3				
• Bahis	3		0	1				2				
• Gezi	0		1	0				2				
Sanatsal Siteler	0	0	2	0	0	0	0	1	0	0	0	0
Portal Siteleri	0	3	0	1	0	0	1	5	0	0	0	0
E-Posta Servis Sağlayıcı Siteler	0	0	0	2	0	0	0	7	0	0	0	0
Toplam	38	14	24	35	0	4	5	108	1	1	1	2

Web sitelerinde captchaların kullanım amacına ve çeşitliliğine göre kullanılan Captcha katmanı bölüm 5.2.'den analiz edilerek oluşturulan Çizelge 4.5. Özet çizelge incelendiğinde; Captcha katmanı olarak incelenen 236 sitede açık ara fark ile en çok tercih edilen reCaptcha Captcha çeşididir. Bunun tercih edilmediği durumlarda daha çok Karmaşık ve Basit Captcha çeşitleri tercih edildiği görülmektedir. En az tercih edilen çeşitleri ise Slider, Güncel, Nesneli captcha ve reCaptcha + Matematik, reCaptcha + Karmaşık, reCaptcha + Resim, Matematik + Karmaşık ikilisinin olduğu görülmektedir.

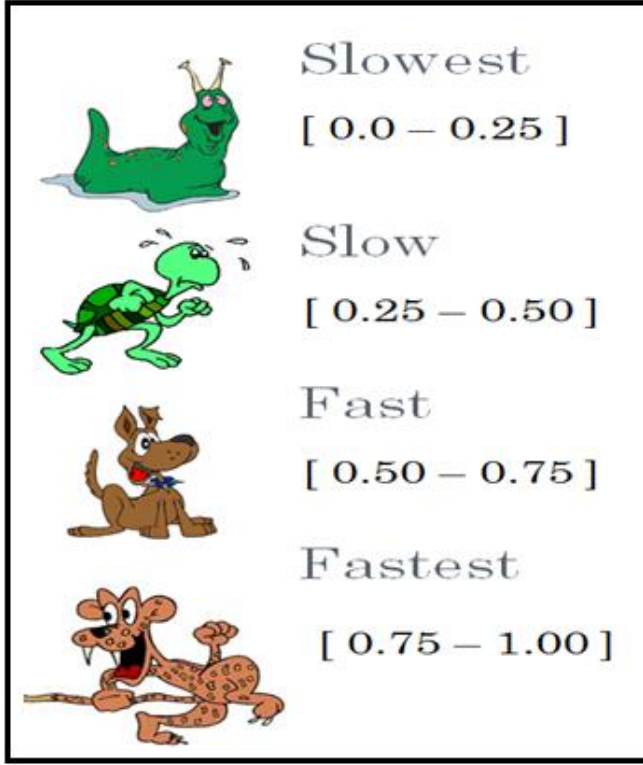
4.4. Kural Tabanlı Algoritmanın Oluşturulması

Klasik mantık küme teorisinde, bir eleman o kümeye aittir veya ait değildir. Ait olduğu elemanına 1 veya 0 değerini atlayarak, o elemanın kendisiyle olan ilişkisini belirtir. Yani nesne 1 değerini alırsa elemanı, 0 değerini alırsa elemanı değildir. Sınırlar keskin olarak belirtilir. Kural tabanlı mantık konusunun temel elemanı kurallı kümedir. Her şey 1 ve 0 arasında derecelendirilir. Bu mantığın hiçbir esnekliği yoktur. Sınırlar keskin olmadığı için belli bir kural çerçevesinde seviyelendirme yapılır.



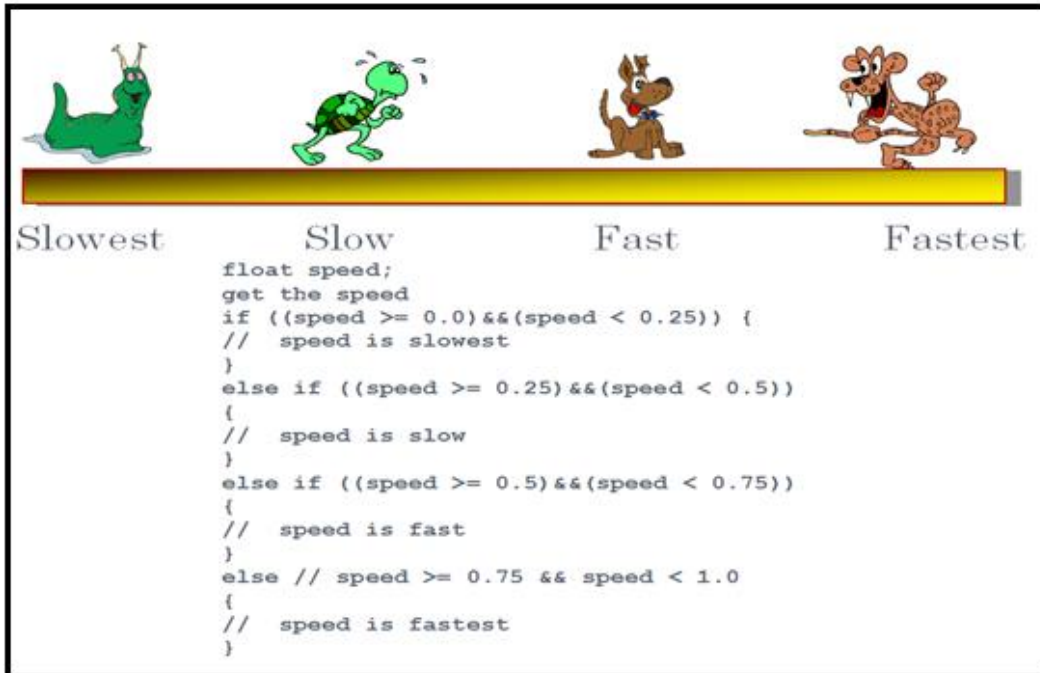
Şekil 4.12. Klasik küme mantık (Warren ve Ballard, 2018)

Şekil 4.12.'de, klasik mantık çerçevesinde yavaş ve hızlı kavramı 1 ve 0 ile temsil edilerek keskin bir ayırım yapılmıştır ve herhangi bir derecelendirmeye tabi tutulmamıştır.



Şekil 4.13. Kural tabanlı küme (Warren ve Ballard, 2018)

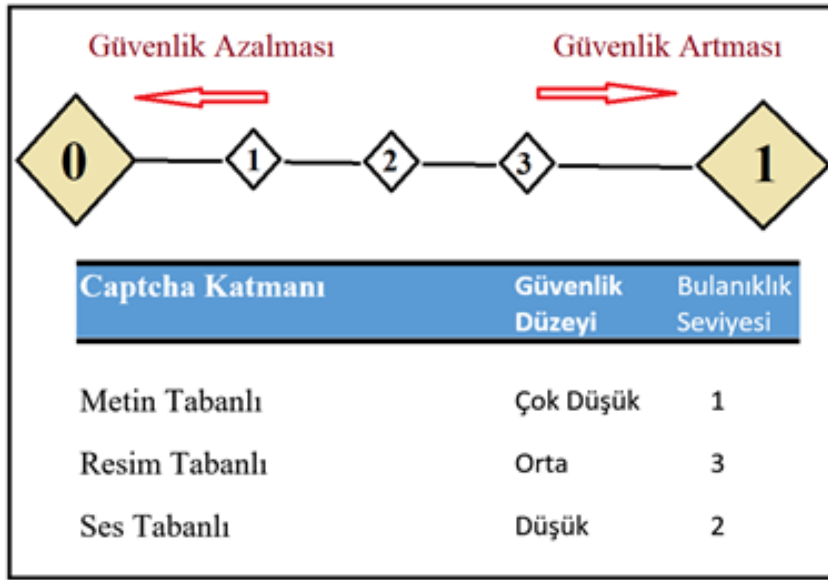
Şekil 4.13.'de, kural tabanı çerçevesinde hız kavramı 0 ve 1 arasında; [0.0 – 0.25], [0.25 – 0.50], [0.50 – 0.75] ve [0.75 – 1.00] olacak şekilde 4 farklı aralıkta temsil edilmiş ve keskin bir ayırım yapmaktan ziyade derecelendirmeye tabi tutmuştur.



Şekil 4.14. Klasik ve kural tabanlı küme mantık (Warren ve Ballard, 2018)

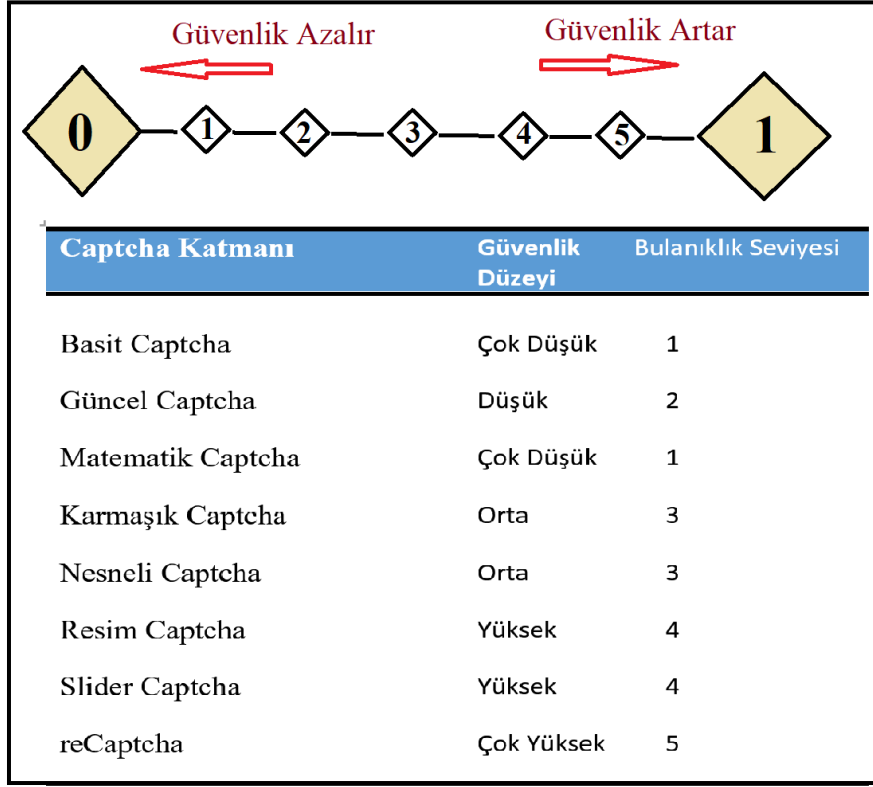
Şekil 4.14.'te, klasik ve kural tabanlı küme mantıkla birlikte ele alındığında; hız kavramı 0 ve 1 arasında $[0.0 - 0.25]$, $[0.25 - 0.50]$, $[0.50 - 0.75]$ ve $[0.75 - 1.00]$ olacak şekilde 4 farklı aralıkta temsil edilmiş olacaktır. Ve bu en yavaş, yavaş, hızlı ve en hızlı gruplandırmıştır.

Kural tabanlı mantık çerçevesinde bu araştırma bulgularının detaylı analizinden pek çok küme oluşturulmuştur. Oluşturulan her kural tabanlı küme kendi içerisinde Captchaların ve katmanlarının kırılma oranlarına göre 1 (güvenli) ve 0 (güvensiz) aralığında belli seviyelerde derecelendirme yapılmıştır. Ya da Captchaların ve katmanlarının kullanılma sıklığına göre (popüler) ve 0 (popüler değil) aralığında kural seviyeleri belirlenmiştir.



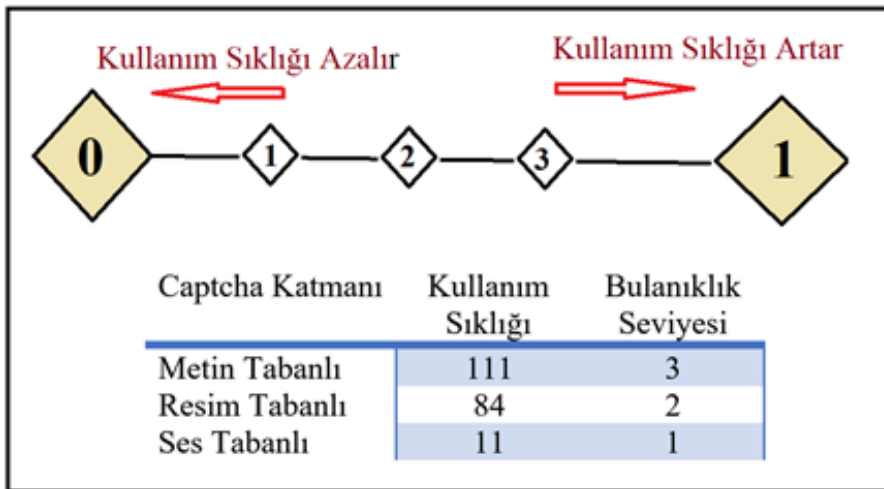
Şekil 4.15. Katman güvenliği kural taban seviyesi

5.1'den elde edilen veriler sonucunda captcha katmanlarının kırılma oranlarına göre güvenlik seviyelerine bağlı kural tabanlı kümesi oluşturulduğunda Şekil 4.15.'deki gibi her güvenlik düzeyine bir seviye verilmiştir. Böylelikle küme 3 elemana sahip olmuştur.



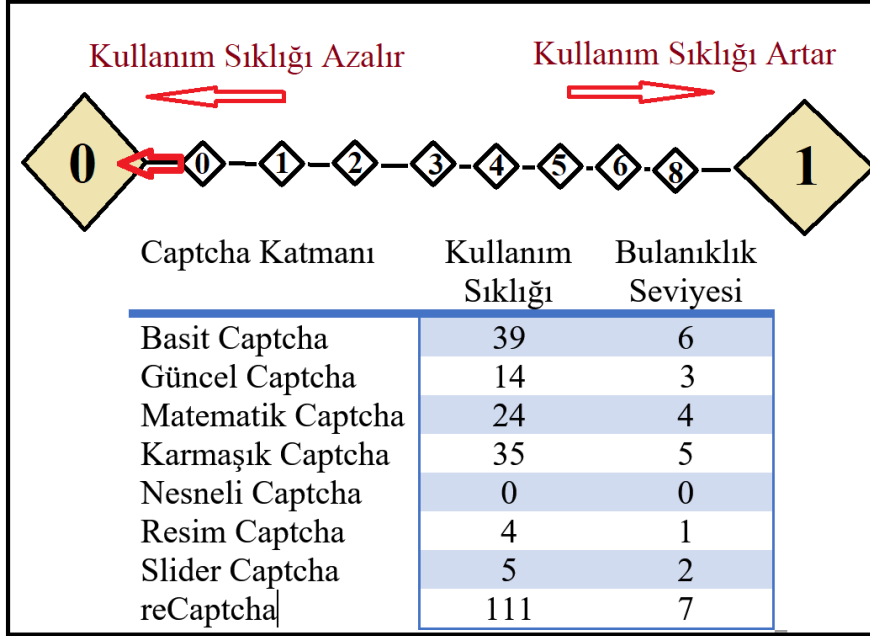
Şekil 4.16. Captcha güvenliği kural taban seviyesi

Bölüm 5.1'den elde edilen veriler sonucunda captcha türlerinin kırılma oranlarına göre güvenlik seviyelerine bağlı kural tabanlı kümesi oluşturulduğunda Şekil 4.16.'daki gibi her güvenlik düzeyine bir seviye verilmiştir. Böylelikle küme 5 elemana sahip olmuştur.



Şekil 4.17. Katman popülerliği kural taban seviyesi

Bölüm 5.4, 5.5 ve 5.6'dan elde edilen veriler sonucunda captcha katmanlarının kullanılma sıklığına bağlı olarak kural tabanlı kümesi oluşturulduğunda Şekil 4.17.'deki gibi her kullanım sıklığında bir seviye verilmiştir. Böylelikle küme 3 elemana sahip olmuştur.



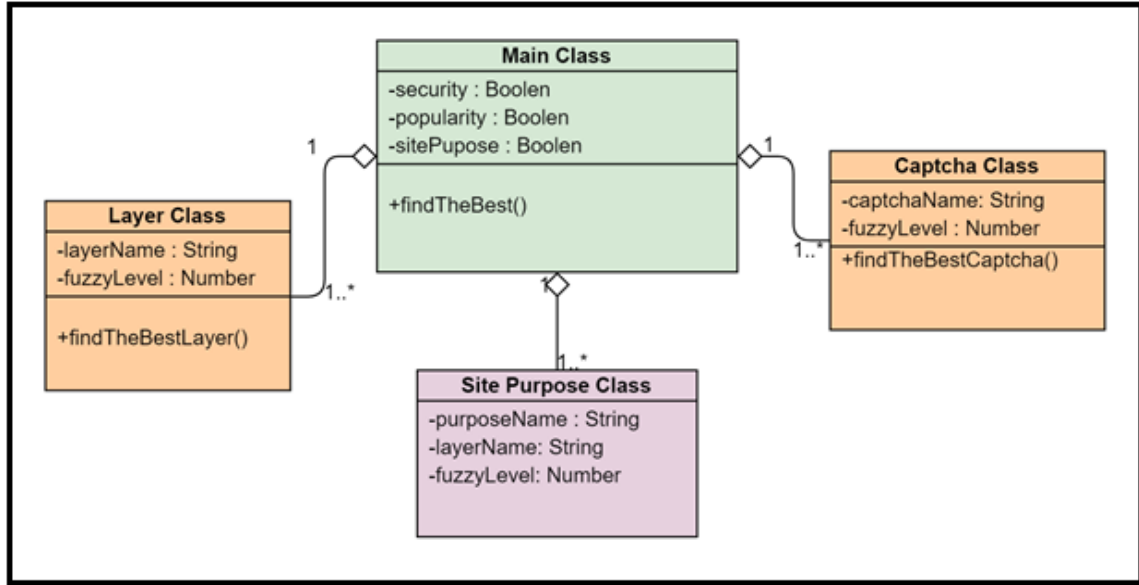
Şekil 4.18. Captcha popülerliği kural taban seviyesi

5.1'den elde edilen veriler sonucunda captcha türlerinin kullanılma sıklığına göre kural tabanlı kümesi oluşturulduğunda Şekil 4.18'deki gibi her kullanım sıklığına bir seviye verilmiştir. Böylelikle küme 8 elemana sahip olmuştur. Nesneli Captcha hiç kullanılmadığı için 0 seviyesi verilmiştir.

Kullanım Amacı	Kullanım Sıklığı Bulanıklık Seviyeleri
Arama Motorları	1, 3
Sosyal Medya Siteleri	2, 7
Haber Siteleri	2, 7
E-Ticaret Siteleri	2, 7
İlan Siteleri	1, 7
Finansal Kurum Siteleri	2, 7
Kişisel Siteler ve Bloglar	1 ve 2, 7
Eğitim Siteleri	2, 7
Firma Siteleri	1, 7 ve 5
Sağlık Siteleri	2, 7 ve 5
Kamu Kurum Siteleri	2, 7
Anket Siteleri	2, 7
Eğlence Siteleri	2, 7
Sanatsal Siteler	1, 4
Portal Siteleri	2, 3
E-Posta Servis Sağlayıcı Siteler	2, 7

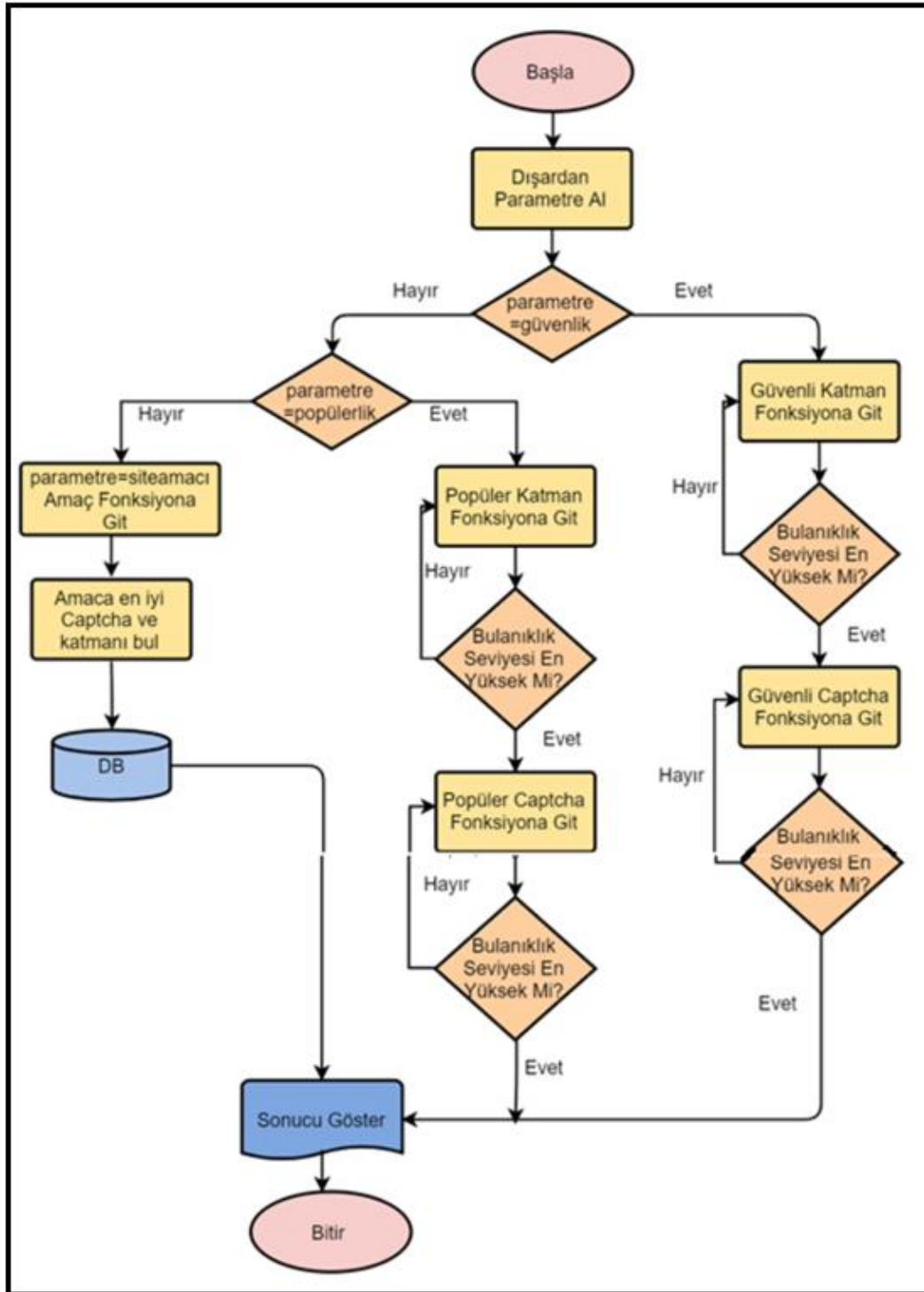
Şekil 4.19. Kullanım amacına göre kural taban seviyesi

İncelenen web sitelerde kullanım amacına göre en çok tercih edilen captcha türü ve katman bilgileri bölüm 5.7’den alınmıştır. Şekil 4.17. ve Şekil 4.18.’den alınan kural tabanlı seviyeleri ile eşleştirilerek en popüler arama katmanı ve captcha seviyeleri Şekil 4.19’de sunulmuştur.



Şekil 4.20. Algoritma sınıfları

Kural tabanlı mantık çerçevesine oluşturulan algoritma temelde Ana sınıf (main class), katman sınıfı (layer class), captcha sınıfı (captcha class) ve siteme amaç sınıfı (site purpose class) olacak şekilde dört ana sınıfa (class) dayanmaktadır. Şekil 4.20’de belirtildiği gibi; katman sınıfının asıl amacı bulgularla elde edilen verilere göre güvenlik ya da popülerlik açısından en uygun katmanı tespit etmektir. Captcha sınıfının görevi bulgularla elde edilen verilere göre güvenlik ya da popülerlik açısından en uygun captcha modeli tespit etmektir. Site amaç sınıfının görevi bulgularla elde edilen verilere göre sadece popülerlik açısından en uygun captcha modeli tespit etmektir. Ana sınıfın amacı da bu üç alt sınıftan elde edilen sonuçlara göre kural tabanı çerçevesinde en uygun sonucu kullanıcıya sunmaktır.



Şekil 4.21. Akış diyagramı

Şekil 4.21.'de görüldüğü gibi algoritma akışı şekilsel olarak sunulmuştur. Dışardan alınan parametre tipine göre akış diyagramı üç ana kola ayrılmaktadır. Parametre tipine göre algoritma akışı otomatik olarak işlemekte ve en uygun sonuç bulununcaya kadar döngüsel halde devam etmektedir. En iyi sonuç, bulgularla elde edilen veri setlerin analiz ve

yorumlanmasına göre oluşturulan veri tabanı baz alınarak bulunmaktadır. Ya da toplanan verilerin kural tabanı çerçevesinde yorumlanmasından oluşan sonuca göre bulunmaktadır. Son adımda da bulunan en uygun sonuç sunulmaktadır.

Çizelge 4.6. Algoritma adımları

1	BAŞLA
2	PARAMETRE SEÇ p_guvenlik="güvenlik", p_populerlik="popülerlik", p_amac="amaç"
3	EĞER parametre==p_guvenlik İSE 4. Adıma GİT, DEĞİLSE 10. Adıma GİT
4	Güvenli Katman Fonksiyona GİT
5	p_guvenliKatmanSeviyesi SEÇ
6	p_guvenliKatmanSeviyesi > Maksimum İSE 7. Adıma GİT DEĞİL İSE 5. Adıma GİT
7	Güvenli Captcha Fonksiyona GİT
8	p_guvenliCaptchaSeviyesi SEÇ
9	p_guvenliCaptchaSeviyesi > Maksimum İSE 20. Adıma GİT DEĞİL İSE 8. Adıma GİT ---
10	EĞER parametre==p_populerlik İSE 11. Adıma GİT, DEĞİLSE 17. Adıma GİT
11	Popüler Katman Fonksiyona GİT
12	p_populerKatmanSeviyesi SEÇ
13	p_populerKatmanSeviyesi > Maksimum İSE 14. Adıma GİT DEĞİL İSE 12. Adıma GİT
14	Popüler Captcha Fonksiyona GİT
15	p_pupulerCaptchaSeviyesi SEÇ
16	p_pupulerCaptchaSeviyesi > Maksimum İSE 20. Adıma GİT DEĞİL İSE 15. Adıma GİT --
17	Amaç Fonksiyona GİT
18	Captcha ve Katman İçin Veri Tabana BAĞLAN
19	Amaca Göre En Uygun Modeli BUL
20	Sonucu Ekrana YAZ
21	BİTİR

4.5. Web Arayüz Geliştirilmesi

Bölüm 4.3. ve 4.4.'den elde edilen verilerin toplanması ve yorumlanması sonucunda Asp.net programlama dili kullanılacak Visual Studio ortamında, web arayüz geliştiricilerin site güvenliği sağlamalarına yardımcı olmak için bir web arayüzü geliştirilmiştir.

Captcha Katmanları Kırılma Durumu	:	☐ Seçiniz	
Captcha Çeşitleri Kırılma Durumu	:	☐ Seçiniz	
Captcha Katmanları Popülerlik Durumu	:	☐ Seçiniz	
Captcha Çeşitleri Popülerlik Durumu	:	☐ Seçiniz	
Web Site Kullanım Amacı	:	Seçiniz	
Captcha Güvenlik	:	☐ Seçiniz	
Captcha Kullanım Sıklığı	:	☐ Seçiniz	
Genel Tablo	:	☐ Seçiniz	
			Göster

Şekil 4.22. Captcha anasayfa(a)

Türkiye’de en çok kullanılan 400 web sitesinin taranıp incelenmesi sonucunda Şekil 4.22.’de görüldüğü gibi oluşturulan web sitesi ile web geliştiricilerine sitelerinde kullanacakları Captcha türünü seçmelerine yardımcı olmaktadır. Ana sayfa kısmında belirtilen seçim kriterleri Captchaların kırılma durumları, popülerlik seviyeleri ve oluşturulan sitenin kullanım amacı gibi üç temel kriter baz alınarak seçimler sunmaktadır. Seçim kriterlerin tamamı bu çalışmada elde edilen verilerin analiz edilmesi ve yorumlanması sonucunda algoritma adımlara dayandırılarak kodlanmıştır.


CAPTCHA



[AnaSayfa](#) [CaptchaBilgi](#) [Açıklama](#) [Hakkında](#)

Uygun Captcha Seçimi

Captcha Katmanları Kırılma Durumu	: ☐ Seçiniz	
Captcha Çeşitleri Kırılma Durumu	: ☒ Seçiniz ✓	
Captcha Katmanları Popülerlik Durumu	: ☐ Seçiniz	
Captcha Çeşitleri Popülerlik Durumu	: ☐ Seçiniz	
Web Site Kullanım Amacı	: Seçiniz	
Captcha Güvenlik	: ☐ Seçiniz	
Captcha Kullanım Sıklığı	: ☐ Seçiniz	
Genel Tablo	: ☐ Seçiniz	

Sonuç Listesi

Satir_Numarasi	Captcha_Cesidi	Güvenlik_Düzeyi
1	reCaptcha	Çok Yüksek
2	Resim Captcha	Yüksek
3	Matematik Captcha	Çok Düşük
4	Karmaşık Captcha	Orta
5	Nesneli Captcha	Orta
6	Güncel Captcha	Düşük
7	Slider Captcha	Yüksek
8	Basit Captcha	Çok Düşük

Şekil 4.23. Captcha anasayfa(b)

Şekil 4.23.'de Captcha çeşidine göre kırılma oranları seçildiğinde 8 Captcha türü, baypas edilebilme durumuna göre güvenlik düzeyleri sıralanmıştır. Böylece güvenlik kriterine dikkat eden web geliştiricilerine seçenekler sunulmuştur. reCaptcha türünün en güvenilir, basit captcha türünün ise en kolay kırılarak baypas edildiği görülmektedir.


CAPTCHA



[AnaSayfa](#) [CaptchaBilgi](#) [Açıklama](#) [Hakkında](#)

Uygun Captcha Seçimi

Captcha Katmanları Kırılma Durumu	Seçiniz	✓	
Captcha Çeşitleri Kırılma Durumu	Seçiniz	✓	
Captcha Katmanları Popülerlik Durumu	Seçiniz		
Captcha Çeşitleri Popülerlik Durumu	Seçiniz		
Web Site Kullanım Amacı	Seçiniz		
Captcha Güvenlik	Seçiniz		
Captcha Kullanım Sıklığı	Seçiniz		
Genel Tablo	Seçiniz		

Sonuç Listesi

Satir_Numarasi	Captcha_Katmani	Captcha
1	Gizli	reCaptcha
2	Görüntü Tabanlı	reCaptcha
3	Ses Tabanlı	reCaptcha
4	Görüntü Tabanlı	Slider Captcha
5	Ses Tabanlı	Slider Captcha
6	Metin Tabanlı	Slider Captcha
7	Görüntü Tabanlı	Resim Captcha
8	Ses Tabanlı	Resim Captcha
9	Metin Tabanlı	Resim Captcha
10	Görüntü Tabanlı	Nesneli Captcha
11	Ses	Nesneli Captcha
12	Metin Tabanlı	Nesneli Captcha
13	Görüntü Tabanlı	Karmaşık Captcha
14	Ses Tabanlı	Karmaşık Captcha
15	Metin Tabanlı	Karmaşık Captcha
16	Görüntü Tabanlı	Güncel Captcha
17	Ses Tabanlı	Güncel Captcha
18	Metin Tabanlı	Güncel Captcha
19	Görüntü Tabanlı	Matematik Captcha
20	Ses Tabanlı	Matematik Captcha
21	Metin Tabanlı	Matematik Captcha
22	Görüntü Tabanlı	Basit Captcha
23	Ses Tabanlı	Basit Captcha
24	Metin Tabanlı	Basit Captcha

Şekil 4.24. Captcha anasayfa(c)

Şekil 4.24.'de kırılma oranlarına göre, captcha türü ve captcha katmanı seçimi yapılmıştır. En güvenli captcha katman ve tür eşleştirilmesi sonucunda güvenlik düzeyine göre en güvenli başlıyarak 24 tane seçenek sunulmuştur. Gizli reCaptcha en güvenli iken metin tabanlı basit captchanın ise en güvensiz seçim olduğu görülmektedir.



CAPTCHA



[AnaSayfa](#)
[CaptchaBilgi](#)
[Açıklama](#)
[Hakkında](#)

Uygun Captcha Seçimi

Captcha Katmanları Kırılma Durumu	: ☐ Seçiniz	
Captcha Çeşitleri Kırılma Durumu	: ☐ Seçiniz	
Captcha Katmanları Popülerlik Durumu	: ☐ Seçiniz	
Captcha Çeşitleri Popülerlik Durumu	: ☐ Seçiniz	
Web Site Kullanım Amacı	: Seçiniz	
Captcha Güvenlik	:	
Captcha Kullanım Sıklığı	:	
Genel Tablo	:	

Sonuç Listesi

Satir_Numarasi	Captcha_Katman	Captcha
1	Görüntü Tabanlı	
2	Gizli	
3	Görüntü Tabanlı	
4	Metin Tabanlı	
5	Metin Tabanlı	
6	Görüntü Tabanlı	
7	Metin Tabanlı	
8	Görüntü Tabanlı	

Göster

Şekil 4.25. Captcha anasayfa(d)

Taranan 400 web sitesi kullanım amacına göre 16 grup halinde ayrı ayrı ele alınıp incelendiği için kullanım amacı kriteri de 16 grup halinde oluşturulmuştur. Bu gruplar çerçevesinde popülerlik ve güvenlik kriterleri sunulmuştur.


CAPTCHA



[AnaSayfa](#)
[CaptchaBilgi](#)
[Açıklama](#)
[Hakkında](#)

Uygun Captcha Seçimi

Captcha Katmanları Kırılma Durumu	:	☐ Seçiniz	
Captcha Çeşitleri Kırılma Durumu	:	☐ Seçiniz	
Captcha Katmanları Popülerlik Durumu	:	☐ Seçiniz	
Captcha Çeşitleri Popülerlik Durumu	:	☐ Seçiniz	
Web Site Kullanım Amacı	:	Eğitim Sitesi	
Captcha Güvenlik	:	☒ Seçiniz	✓
Captcha Kullanım Sıklığı	:	☐ Seçiniz	
Genel Tablo	:	☐ Seçiniz	

Sonuç Listesi

Satir_Numarasi	Captcha_Katmani	Captcha_Cesidi
1	Gizli	reCaptcha
2	Görüntü Tabanlı	Karmaşık Captcha
3	Görüntü Tabanlı	Matematik ve Karmaşık Captcha
4	Metin Tabanlı	Matematik Captcha
5	Görüntü Tabanlı	Basit Captcha
6	Metin Tabanlı	Basit Captcha

Şekil 4.26. Captcha anasayfa(e)

Şekil 4.26.'da Captcha modelin kullanılacağı web sitenin Eğitim Sitesi olduğu ve güvenlik kriteri seçilmiştir. Eğitim sitelerinde kullanılan captchaların kırılma oranları dikkate alınarak sıralama yapıldığında, en çok gizli reCaptcha tercih edilirken en az ise kolaylıkla baypas edilebilen metin tabanlı basit captcha olduğu görülmektedir.


CAPTCHA



[AnaSayfa](#) [CaptchaBilgi](#) [Açıklama](#) [Hakkında](#)

Uygun Captcha Seçimi

Captcha Katmanları Kırılma Durumu	:	☐ Seçiniz	
Captcha Çeşitleri Kırılma Durumu	:	☐ Seçiniz	
Captcha Katmanları Popülerlik Durumu	:	☐ Seçiniz	
Captcha Çeşitleri Popülerlik Durumu	:	☐ Seçiniz	
Web Site Kullanım Amacı	:	Eğitim Sitesi	
Captcha Güvenlik	:	☒ Seçiniz	✓
Captcha Kullanım Sıklığı	:	☒ Seçiniz	✓
Genel Tablo	:	☐ Seçiniz	

Sonuç Listesi

Satir_Numarasi	Captcha_Katmani	Captcha_Cesidi
1	Gizli	reCaptcha
2	Metin Tabanlı	Basit Captcha
3	Görüntü Tabanlı	Karmaşık Captcha
4	Metin Tabanlı	Matematik Captcha

Şekil 4.27. Captcha anasayfa(f)

Eğitim sitelerinde güvenlik ve popülerlik kriterlerine göre sıralanma istendiğinde, Şekil 4.27.'de görüldüğü gibi gizli reCaptcha, metin tabanlı basit captcha, görüntü tabanlı karmaşık captcha ve metin tabanlı matematik captcha seçimleri sunulmuştur.

CAPTCHA

[AnaSayfa](#)
[CaptchaBilgi](#)
[Açıklama](#)
[Hakkında](#)

Uygun Captcha Seçimi

Captcha Katmanları Kırılma Durumu	: Seçiniz	
Captcha Çeşitleri Kırılma Durumu	: Seçiniz	
Captcha Katmanları Popülerlik Durumu	: Seçiniz	
Captcha Çeşitleri Popülerlik Durumu	: Seçiniz	
Web Site Kullanım Amacı	: Seçiniz	
Captcha Güvenlik	: Seçiniz	
Captcha Kullanım Sıklığı	: ☒ Seçiniz	✓
Genel Tablo	: Seçiniz	

Sonuç Listesi

Satir_Numarası	Captcha_Katmanı	Captcha
1	Görüntü Tabanlı	reCaptcha
2	Gizli	reCaptcha
3	Görüntü Tabanlı	Basit Captcha
4	Metin Tabanlı	Basit Captcha
5	Metin Tabanlı	Karmaşık Captcha
6	Görüntü Tabanlı	Karmaşık Captcha
7	Metin Tabanlı	Matematik Captcha
8	Görüntü Tabanlı	Matematik Captcha
9	Metin Tabanlı	Güncel Captcha
10	Görüntü Tabanlı	Güncel Captcha
10	Görüntü Tabanlı	Slider Captcha
11	Metin Tabanlı	Slider Captcha
12	Görüntü Tabanlı	Resim Captcha
13	Görüntü Tabanlı	Nesneli Captcha
14	Metin Tabanlı	Nesneli Captcha

Şekil 4.28. Captcha anasayfa(g)

Bulgular bölümünde taranan 400 web sitesi popülerlik durumuna göre captcha katman ve türlerin kullanım durumları incelenmiş ve analizi yapılmıştı. Bu tespit sonucunda Şekil 4.28.'de görüldüğü gibi sadece popülerlik durumu seçildiğinde 14 seçenek ile öneriler verilmiştir. En popüler türlerin reCaptcha ve basit captcha olduğu, en az tercih edilen captcha türlerin ise nesneli captcha olduğu görülmektedir.


CAPTCHA



[AnaSayfa](#)
[CaptchaBilgi](#)
[Açıklama](#)
[Hakkında](#)

Uygun Captcha Seçimi

Captcha Katmanları Kırılma Durumu	: ☐ Seçiniz	
Captcha Çeşitleri Kırılma Durumu	: ☐ Seçiniz	
Captcha Katmanları Popülerlik Durumu	: ☐ Seçiniz	
Captcha Çeşitleri Popülerlik Durumu	: ☐ Seçiniz	
Web Site Kullanım Amacı	: Seçiniz	
Captcha Güvenlik	: ☐ Seçiniz	
Captcha Kullanım Sıklığı	: ☐ Seçiniz	
Genel Tablo	: ☒ Seçiniz	

Sonuç Listesi

Satir_Numarası	Captcha_Katmanı	Captcha_Cesidi	Güvenlik_Seviyesi	Popülerlik_Seviyesi
1	Gizli	reCaptcha	1	1
2	Görüntü Tabanlı	reCaptcha	2	2
3	Ses Tabanlı	reCaptcha	3	3
4	Görüntü Tabanlı	Slider Captcha	4	17
5	Ses Tabanlı	Slider Captcha	5	18
6	Metin Tabanlı	Slider Captcha	6	16
7	Görüntü Tabanlı	Resim Captcha	7	20
8	Ses Tabanlı	Resim Captcha	8	21
9	Metin Tabanlı	Resim Captcha	9	19
10	Görüntü Tabanlı	Nesneli Captcha	10	23
11	Ses	Nesneli Captcha	11	24
12	Metin Tabanlı	Nesneli Captcha	12	22
13	Görüntü Tabanlı	Karmaşık Captcha	13	8
14	Ses Tabanlı	Karmaşık Captcha	14	9
15	Metin Tabanlı	Karmaşık Captcha	15	7
16	Görüntü Tabanlı	Güncel Captcha	16	14
17	Ses Tabanlı	Güncel Captcha	17	15
18	Metin Tabanlı	Güncel Captcha	18	13
19	Görüntü Tabanlı	Matematik Captcha	19	11
20	Ses Tabanlı	Matematik Captcha	20	12
21	Metin Tabanlı	Matematik Captcha	21	10
22	Görüntü Tabanlı	Basit Captcha	22	5
23	Ses Tabanlı	Basit Captcha	23	6
24	Metin Tabanlı	Basit Captcha	24	4

Şekil 4.29. Captcha anasayfa(h)

Popülerlik, güvenlik düzeyi, captcha türü ve katmanları ile genel bir tablo oluşturulduğunda Şekilde 4.29.'daki sonuçlara varılmıştır. En popüler ve güvenli captcha çeşidinin gizli reCaptcha olduğu görülmektedir. Metin tabanlı basit captcha popüler açısından üst sıralarda iken güvenlik seviyesi açısından sonlarda olduğu görülmektedir.




[AnaSayfa](#)
[CaptchaBilgi Açıklama](#)
[Hakkında](#)

Captcha Dünyasında Hoş Geldiniz!

Siber dünyada, teknoloji ve internetin hızla ilerlemesi beraberinde geliştirmekte olan siber suçları da getirmektedir. Captcha Çeşitliliği bu suçları engellemek amacıyla oluşturulan bir güvenlik katmanı olarak bilini

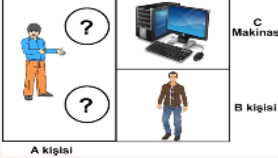
Completely
Automated
Public
Turing test to tell
Computers and
Humans
Apart

➔

CAPTCHA

Turing Test

İlk olarak 1950 yılında Alan Turing Computing Machinery and Intelligence isimli makalesinde değinmiştir. Turing Testinin amacı bir bilgisayarın düşündüğünü söyleyebilmenin mümkün olup olmayacağıdır. Turing testine göre sorgulayıcının soru sorması suretiyle, yöneltilen sorulara cevap verenlerden hangisinin bilgisayar hangisinin insan olduğunu saptamaya çalışmasıdır. Sorgulayıcının soruları sadece bir klavye aracılığıyla yazılarak gönderilmektedir. Tekrarlanan testler sonucunda sorgulayıcı, cevap vericinin insan olup olmadığını saptayamadığı takdirde bilgisayar Turing Testini geçmiş sayılmaktadır



Captcha temelde tek katmanlı ve iki katmanlı olarak ikiye ayrılmıştır:

- 1- Tek katmanlı Captcha**
 - Metin tabanlı Görüntü tabanlı ve
 - Ses tabanlı olarak üç kategoriye ayrılabilir.
- 2- İki Katmanlı Captcha**
 - Metin, görüntü ve ses tabanlı captchaların ikili kombinasyonların oluşur.

Captcha Çeşitleri:

- 1- Basit Captcha
- 2- Matematik Captcha
- 3- Nesneli Captcha
- 4- Resim Captca
- 5- Güncel Captcha
- 6- Slider Captcha
- 7- Karmaşık Captcha
- 8- reCaptcha

en çok tercih edilen captcha modelleridir.

Captcha katmanları ve çeşitleri ile ilgili detaylı bilgiyi aşağıdaki makalden bulabilirsiniz.

Makale erişme linki: <https://j-humansciences.com/ojs/index.php/IJHS/article/view/5201/2585>



Journal of Human Sciences
ISSN: 2458-9489
Volume 15 Issue 3 Year: 2018

Robust security against cyber threats with variety of captcha

Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması

Hüseyin Çakır¹
Necla Ulubatuo²

Abstract
Cyberpace also brings about cybercrime, which is evolving along with the rapid progress of technology and internet. Captchas are used as a layer of security to prevent these crimes. It is a security mechanism designed to distinguish whether an entry is made by the user when entering a system and is used for protection against malicious bot programs. For this reason, it is important that the introduction is done by

Özet
Siber dünyada, teknoloji ve internetin hızla ilerlemesi beraberinde geliştirmekte olan siber suçları da getirmektedir. Güvenlik kodları (captcha) bu suçları engellemek amacıyla oluşturulan bir güvenlik katmanı olarak kullanılmaktadır. Bir sisteme giriş yapıldığında girilen kullanıcı tarafından yapılabildiği kadar güvenli bir şekilde kullanılması için tasarlanmış bir güvenlik mekanizması ve kötü niyetli bot programlarına karşı koruma amaçlı kullanılır. Bu

Şekil 4.30. Captcha anasayfa(i)

Captcha Bilgi sayfasında ise kullanıcılara captchalarla ilgili genel bilgiler verilmiştir.

5. BULGULAR VE YORUM

Bu bölümde çalışma boyunca elde edilen bulgular ve bulgu sonuçlara göre yorumlar ele alınmıştır.

5.1. Captchaların Kırılma Oranlarına Göre İncelenmesi

Yayınlanmış ulusal, uluslararası makalelerden ve teknolojik haberlerinden elde edilen bilgiler doğrultusunda Captcha modelleri ve kırılma oranlarını gösteren 5.1. ve 5.2. çizelgeleri oluşturulmuştur. Çizelgelerde belirtilen değerler en az yirmi tane yayınlanmış ulusal, uluslararası makale incelenerek elde edilmiştir. Birçok teknoloji sitesindeki güncel haberler de incelemeye dâhil edilmiştir.

Çizelge 5.1. Captcha katmanlarında kırılmaların karşılaştırması

Captcha Katmanı	İnsan Kaynaklı İstismar	OCR Çözümü	Yapay Sinir Ağları ile Kırılmış Mı?	Güvenlik Düzeyi
Metin Tabanlı	Var	Var	Evet	Çok Düşük
Resim Tabanlı	Var	Yok	Evet	Orta
Ses Tabanlı	Var	Yok	Evet	Düşük

Çizelge 5.1. de görüldüğü üzere Captcha katmanları arasında karşılaştırmalı gruplandırma yapıldığında kullanılan katmanların sürekli gelişmekte olan teknolojiye ayak uyduramadığı görülmektedir. Resim tabanlı Captcha katmanının metin ve ses katmanına göre daha güçlü bir güvenlik seviyesinin olduğu görülmektedir.

Çizelge 5.2. Captcha türünde kırılmaların karşılaştırması

Captcha Türü	Captcha Türü Kırılmış Mı?	OCR Çözümü	Yapay Sinir Ağları ile Kırılmış Mı?	Güvenlik Düzeyi
Basit Captcha	Evet	Var	Evet	Çok Düşük
Güncel Captcha	Evet	Var	Evet	Düşük
Matematik Captcha	Evet	Var	Evet	Çok Düşük
Karmaşık Captcha	Evet	Var	Evet	Orta
Nesneli Captcha	Evet	Yok	Evet	Orta
Resim Captcha	Evet	Yok	Evet	Yüksek
Slider Captcha	Evet	Yok	Evet	Yüksek
reCaptcha	Hayır	Yok	Hayır	Çok Yüksek

Çizelge 5.2.'deki veriler incelendiğinde, Captcha Türü Kırılmaların Karşılaştırmasından elde edilen veriler görülmektedir. Bu veriler doğrultusunda inceleme yapıldığında en güvenilir Captcha türünün reCaptcha olduğu görülmektedir.

Basit ve matematik Güvenlik kodların (Captcha) ise gruplandırmada en güvensiz oldukları görülmektedir. Çizelgeden de anlaşıldığı üzere gelişen teknolojiye ayak uyduran ve karmaşıklık ve katman çokluğu içeren Güvenlik kodların (Captcha) diğerlerine kıyasla da güvenilir olduğu anlaşılmaktadır.

5.2. Web Site Amacına Göre Captchaların İncelenmesi

Web sitelerin kullanım amaçlarına göre ana ve alt gruplar oluşturularak incelenmiştir. İncelenen web siteleri ele alınırken; en çok tercih edilen popüler siteler ve arama motorlarında en üst sıralarda çıkmış olanlar daha çok tercih edilmiştir.

5.2.1. Arama motorları

Çizelge 5.3. oluşturulurken Alexa verilerine göre en çok kullanılan arama motorları baz alınarak inceleme yapılmıştır.

Arama motorlarında Captcha görülmesi yok denecek kadar azdır. Genellikle olağandışı trafik etkinlikleri tespit ettiğinde Captcha mesajı görülmektedir. Olağandışı etkinlik durdurulduktan sonra arama motorları normal olarak arama yapılmasına izin verir.

Çizelge 5.3. Arama motorları

	İncelenen Arama Motoru	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Google	Evet	reCaptcha	Resim Katmanlı
2	Yahoo	Evet	Güncel Captcha	Metin Tabanlı
3	Yandex	Evet	Güncel Captcha	Metin Tabanlı
4	Bing	Evet	Güncel Captcha	Metin Captcha
5	Ask	Hayır	Yok	Yok
6	Baidu	Evet	Güncel Captcha	Metin Captcha
7	Yaani	Hayır	Yok	Yok
8	AOL Search	Hayır	Yok	Yok
9	DuckDuckGo	Evet	Basit Captcha	Metin Tabanlı
10	GoodSearch	Evet	Basit Captcha	Metin Tabanlı
11	InfoSpace.com	Hayır	Yok	Yok
12	Info.com	Hayır	Yok	Yok
13	BoardReader	Hayır		
14	MyWebSearch	Evet	Basit Captcha	Metin Tabanlı
15	DogPile	Hayır	Yok	Yok

Çizelge 5.3. verileri incelendiğinde arama motorlarında Captcha türü olarak daha çok Güncel Captcha'nın tercih edildiği görülmektedir. Arama motoru devri olarak bilinen Google'nin, kendisinin üretmiş olduğu reCaptcha tercih ettiğini görmekteyiz. Basit Captcha kullanan veya Captcha kullanmayan arama motorların daha çok diğer büyük arama motorlarının veri havuzundan beslendiğini araştırma sonucunda tespit edilmiştir. Örneğin: MyWebSearch; Google veri havuzunu, DogPile; Google ve Yahoo veri havuzunu, GoodSearch; Yahoo veri

havuzundan yararlanmaktadır. Çizelge verilerine genel olarak bakıldığında Captcha tercih etmeyen arama motorların da çoğunlukta olduğu görülmektedir.

5.2.2. Sosyal medya siteleri

Çizelge 5.4. oluşturulurken Alexa verilerine göre en çok kullanılan sosyal medya siteleri baz alınarak inceleme yapılmıştır



Çizelge 5.4. Sosyal medya siteleri

	İncelenen Sosyal Medya	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Facebook	Evet	Resim Captcha	Resim Tabanlı
2	Google+	Evet	reCaptcha	Resim Tabanlı
3	Twitter	Evet	reCaptcha	Resim Tabanlı
4	Instagram	Evet	Resim Captcha	Resim Tabanlı
5	Swarm	Evet	Resim Captcha	Resim Tabanlı
6	LinkedIn	Evet	Güncel Captcha	Metin Tabanlı
7	Badoo	Evet	Güncel Captcha	Metin Tabanlı
8	Youtube	Evet	reCaptcha	Resim Tabanlı
9	Spotify	Evet	reCaptcha	Resim Tabanlı
10	Apple Music	Evet	Güncel Captcha	Metin Tabanlı
11	RottenTomatoes	Evet	reCaptcha	Resim Tabanlı
12	Last.fm	Evet	reCaptcha	Resim Tabanlı
13	Fotolog	Evet	reCaptcha	Resim Tabanlı
14	LiveJournal	Evet	reCaptcha	Resim Tabanlı
15	FourSquare	Evet	reCaptcha	Resim Captcha
16	Xing	Hayır	Yok	Yok
17	StumbleUpon	Evet	reCaptcha	Resim Tabanlı
18	Tumblr	Evet	reCaptcha	Resim Tabanlı
19	Pinterest	Evet	Resim Captcha	Resim Tabanlı
20	DailyMation	Evet	reCaptcha	Resim Tabanlı
21	Fizy	Hayır	Yok	Yok

Çizelge 5.4. verileri incelendiğinde sosyal medya sitelerinde Captcha türü olarak daha çok reCaptcha'nın tercih edildiği görülmektedir. Facebook, Instagram, Swarm ve Pinterest gibi popüler uygulamaların daha çok Resim Captcha tercih ettiğini görmekteyiz. Çizelge genel olarak incelendiğinde sosyal medya sitelerinin çoğunun bir Captcha türünü tercih ettiğini görmekteyiz.

5.2.3. Haber siteleri

Arama motorlarında tarama yapıldığında en çok tercih edilen haber siteleri statüsüne sahip web siteler baz alınarak incelemeye alınmıştır.

Yerel haber siteleri

Yerel haber siteleri tarama grubuna dahil edilirken daha çok büyük şehir yerel haber web siteleri tercih edilmiştir.

Çizelge 5.5. Yerel haber siteleri

	İncelenen Yerel Haber Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Ankara Haber	Evet	Matematik Captcha	Metin Tabanlı
2	İstanbul Haber	Evet	Basit Captcha	Metin Tabanlı
3	İzmir Habercisi	Hayır	Yok	Yok
4	Adana Haber Merkezi	Evet	Matematik Captcha	Metin Tabanlı
5	Bursa.com	Hayır	Yok	Yok
6	Gündem Van	Evet	reCaptcha	Resim Tabanlı
7	Eskisehir.net	Evet	reCaptcha	Resim Tabanlı
8	Kayserinews.com	Evet	Basit Captcha	Metin Tabanlı
9	Trabzon haber61	Evet	Matematik Captcha	Metin Tabanlı
10	Antalya gazetealanya.com	Evet	Matematik Captcha	Metin Tabanlı

Çizelge 5.5. verileri incelendiğinde yerel haber sitelerinde Captcha türü olarak daha çok Matematik Captcha'nin tercih edildiği görülmektedir. Çizelge verilerine genel olarak bakıldığında yerel haber sitelerinde sistematik bir Captcha kullanımının olmadığı görülmektedir.

Ulusal haber siteleri

Ulusal haber siteleri tarama grubuna dahil edilirken arama motorlarında en üstte çıkan ya da en popüler olan ulusal web siteler tercih edilmiştir.

Çizelge 5.6. Ulusal haber siteleri

	İncelenen Ulusal Haber Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Hürriyet	Evet	reCaptcha	Resim Tabanlı
2	Sözcü	Evet	reCaptcha	Resim Tabanlı
3	Sabah	Evet	reCaptcha	Resim Tabanlı
4	Milliyet	Hayır	Yok	Yok
5	Cumhuriyet	Hayır	Yok	Yok
6	HaberTürk	Evet	reCaptcha	Resim Tabanlı
7	Onedio	Evet	reCaptcha	Resim Tabanlı
8	Posta	Hayır	Yok	Yok
9	Akşam	Hayır	Yok	Yok
10	Fanatik	Hayır	Yok	Yok

Çizelge 5.6. verileri incelendiğinde ulusal haber sitelerinde Captcha türü olarak daha çok reCaptcha'nin tercih edildiği görülmektedir. Çizelge verilerine genel olarak bakıldığında ulusal haber sitelerinde Captcha kullanımının pek tercih edilmediği görülmektedir.

Uluslararası haber siteleri

Uluslararası haber siteleri tarama grubuna dahil edilirken arama motorlarında en üstte çıkan ya da en popüler olan uluslararası web siteleri tercih edilmiştir.

Çizelge 5.7. Uluslararası haber siteleri

	İncelenen Uluslararası Haber Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	CNBC	Evet	reCaptcha	Resim Tabanlı
2	BBC	Evet	reCaptcha	Resim Tabanlı
3	CNN	Evet	reCaptcha	Resim Tabanlı
4	JapanTimes	Hayır	Yok	Yok
5	WashingtonTimes	Evet	reCaptcha	Resim Tabanlı
6	EuroNews	Evet	reCaptcha	Resim Tabanlı
7	NYTimes	Evet	reCaptcha	Resim Tabanlı
8	El Cezire	Evet	reCaptcha	Resim Tabanlı
9	Pravda	Evet	reCaptcha	Resim Tabanlı
10	FarsNews	Evet	reCaptcha	Resim Tabanlı

Çizelge 5.7. verileri incelendiğinde uluslararası haber sitelerinde Captcha türü olarak daha çok reCaptcha'nın tercih edildiği görülmektedir. Uluslararası haber sitelerin diğer haber sitelerine göre Captcha kullanımının daha yaygın olduğunu görmekteyiz.

5.2.4. E-ticaret siteleri

Arama motorlarında tarama yapıldığında en çok tercih edilen e-ticaret siteleri statüsüne sahip web siteler baz alınarak incelemeye alınmıştır.

B2B siteleri

B2B siteleri (business to business, firmadan firmaya)ticaret siteleri tarama grubuna dahil edilirken arama motorlarında en üstte çıkan ya da en popüler olan B2B web siteler tercih edilmiştir.

Çizelge 5.8. B2B siteleri

	İncelenen B2B Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Alibaba	Evet	Slider Captcha	Metin Tabanlı
2	Kompass	Evet	reCaptcha	Resim Tabanlı
3	TradeTurkey	Hayır	Yok	Yok
4	Türk Ticaret	Evet	reCaptcha	Resim Tabanlı
5	Amazon	Evet	Güncel Captcha	Metin Tabanlı
6	RusBiz	Hayır	Yok	Yok
7	EC21	Evet	reCaptcha	Resim Tabanlı
8	GlobalSource	Hayır	Yok	Yok
9	PayPal	Hayır	Yok	Yok
10	turkfreezone	Hayır	Yok	Yok

Çizelge 5.8. verileri incelendiğinde B2B sitelerinde Captcha türü olarak daha çok reCaptcha'nın tercih edildiği görülmektedir. B2B sitelerinde Captcha kullanımının pek yaygın olmadığı görülmektedir.

B2C siteleri

B2C Siteleri (business to customer, firmadan müşteriye) ticaret siteleri tarama grubuna dahil edilirken arama motorlarında en üstte çıkan ya da en popüler olan B2C web siteler tercih edilmiştir.

Çizelge 5.9. B2C siteleri

	İncelenen B2C Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Alibaba	Evet	Slider Captcha	Metin Tabanlı
2	Ebay	Hayır	Yok	Yok
3	Amazon	Evet	Güncel Captcha	Metin Tabanlı
4	PayPal	Hayır	Yok	Yok
5	N11	Hayır	Yok	Yok
6	Hepsiburada	Evet	Karmaşık Captcha	Metin Tabanlı
7	Trendyol	Hayır	Yok	Yok
8	Limango	Hayır	Yok	Yok
9	Biletix	Hayır	Yok	Yok
10	Tatil	Hayır	Yok	Yok

Çizelge 5.9. verileri incelendiğinde B2C sitelerinde Captcha kullanımının pek yaygın olmadığı görülmektedir. Captcha kullanan B2C sitelerinde daha çok metin tabanlı Captcha katmanı tercih edildiği görülmektedir.

C2C siteleri

C2C Siteleri (customer to customer, müşteriden müşteriye) ticaret siteleri tarama grubuna dahil edilirken arama motorlarında en üstte çıkan ya da en popüler olan C2C web siteler tercih edilmiştir.

Çizelge 5.10. C2C siteleri

	İncelenen C2C Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Alibaba	Evet	Slider Captcha	Metin Tabanlı
2	Ebay	Hayır	Yok	Yok
3	Sahibinden	Evet	Güncel Captcha	Metin Tabanlı
4	GittiGidiyor	Evet	reCaptcha	Resim Tabanlı
5	LetGo	Evet	reCaptcha	Resim Tabanlı
6	Dolap..com	Evet	reCaptcha	Resim Tabanlı
7	PayPal	Hayır	Yok	Yok
8	Etsy	Evet	reCaptcha	Resim Tabanlı
9	Bonanza	Hayır	Yok	Yok
10	Arabam.com	Evet	reCaptcha	Resim Tabanlı

Çizelge 5.10. verileri incelendiğinde C2C sitelerinde Captcha türü olarak daha çok reCaptcha'nın tercih edildiği görülmektedir.C2C sitelerinde Captcha kullanımının B2B ve B2C göre daha çok tercih edilir olduğu görülmektedir.

5.2.5. İlan siteleri

İlan siteleri incelenirken; arama motorlarında tarama yapıldığında en çok tercih edilen ilan web siteleri statüsüne sahip siteler baz alınarak incelemeye alınmıştır.

Çizelge 5.11. İlan siteleri

	İncelenen İlan Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	HürriyetEmlak	Evet	reCaptcha - Karmaşık Captcha	Resim Tabanlı - Metin Tabanlı
2	Sahibinden.com	Evet	Basit Captcha	Metin Tabanlı
3	Waa2	Hayır	Yok	Yok
4	İlanExpress	Evet	Karmaşık Captcha	Metin Tabanlı
5	Memurlar.Net	Evet	Karmaşık Captcha	Resim Tabanlı
6	DoD	Hayır	Yok	Yok
7	Booking.com	Evet	reCaptcha	Resim Tabanlı
8	Kariyer.net	Evet	reCaptcha	Resim Tabanlı
9	İşKur	Evet	Basit Captcha	Metin Tabanlı
10	İlan.gov.tr	Evet	Basit Captcha	Metin Tabanlı

Çizelge 5.11. verileri incelendiğinde ilan sitelerinde Captcha türü olarak daha çok Basit Captcha'nin tercih edildiği görülmektedir. Çizelge verileri yorumlandığında C2C sitelerinde Captcha kullanımının B2B ve B2C göre daha çok tercih edilir olduğu ve Resim Tabanlı Captcha'ların tercih edildiği sonucuna varılmaktadır.

5.2.6. Finansal kurum siteleri

Arama motorlarında tarama yapıldığında en çok tercih edilen finansal kurum siteleri statüsüne sahip siteler baz alınarak incelemeye alınmıştır.

Banka siteleri

Banka siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen banka siteleri statüsüne sahip siteler baz alınarak gruba alınmıştır.

Çizelge 5.12. Banka siteleri

	İncelenen Banka Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	ING	Evet	Karmaşık Captcha	Metin ve Ses Tabanlı
2	Akbank	Evet	Karmaşık Captcha	Resim ve Ses Tabanlı
3	YapıKredi	Evet	Güncel Captcha	Metin ve Ses Tabanlı
4	VakıfBank	Evet	Basit Captcha	Metin ve Ses Tabanlı
5	DenizBank	Evet	Karmaşık Captcha	Resim ve Ses Tabanlı
6	GarantiBank	Evet	Karmaşık Captcha	Metin ve Ses Tabanlı
7	Ziraat	Evet	Basit Captcha	Metin ve Ses Tabanlı
8	HSBC	Evet	Karmaşık Captcha	Metin Tabanlı
9	İşBank	Evet	Basit Captcha	Metin Tabanlı
10	HalkBank	Evet	reCaptcha	Resim Tabanlı

Çizelge 5.12. verileri incelendiğinde banka sitelerinde Captcha türü olarak daha çok Karmaşık Captcha'nın tercih edildiği görülmektedir. Çizelge verileri yorumlandığında

banka sitelerinde Metin ve Ses tabanlı Captcha kullanımının daha yaygın olduğu sonucuna varılmaktadır. Captcha kullanımının yanında cep telefon kodu (Gsm-code) da kullanılmaktadır.

Borsa siteleri

Borsa siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen borsa siteleri statüsüne sahip siteler baz alınarak gruba alınmıştır.

Çizelge 5.13. Borsa siteleri

	İncelenen Borsa Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	BorsaDirect	Evet	reCaptcha	Resim Tabanlı
2	Gcmforex	Hayır	Yok	Yok
3	Foreks	Hayır	Yok	Yok
4	Borsaİstanbul	Evet	Basit Captcha	Metin Tabanlı
5	Investing	Evet	reCaptcha	Resim Tabanlı
6	Binomo	Evet	reCaptcha	Resim Tabanlı
7	Döviz	Hayır	Yok	Yok
8	BloomBerg	Evet	Karmaşık Captcha	Metin Tabanlı
9	Fool	Hayır	Yok	Yok
10	Street	Hayır	Yok	Yok

Çizelge 5.13. verileri incelendiğinde borsa sitelerinde Captcha kodu kullanımı pek tercih edilmediği görülmektedir. Çizelge verileri yorumlandığında borsa sitelerinde daha çok herkese açık anlık güncel bilgi paylaşımı yapıldığı için tercih edilmediği sonucuna varılabilir. Veri girişi gerektiren borsa sitelerinde daha çok cep telefon kodu (gsm-code) kullanılmaktadır.

Kripto para siteleri

Kripto para siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen kripto para siteleri statüsüne sahip siteler baz alınarak gruba alınmıştır.

Çizelge 5.14. Kripto para siteleri

	İncelenen Kripto Para Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Paribu	Hayır	Yok	Yok
2	Koinim	Evet	reCaptcha	Resim Tabanlı
3	BiTürk	Evet	reCaptcha	Resim Tabanlı
4	UzmanCoin	Hayır	Yok	Yok
5	bitci	Evet	reCaptcha	Resim Tabanlı
6	Coinbase	Evet	reCaptcha	Resim Tabanlı
7	Coinmama	Evet	reCaptcha	Resim Tabanlı
8	Hitbtc	Evet	reCaptcha	Resim Tabanlı
9	Kraken	Evet	reCaptcha	Resim Tabanlı
10	Binance	Evet	Slide Captcha	Resim Tabanlı

Çizelge 5.14. verileri incelendiğinde kripto para sitelerinde Captcha türü olarak daha çok reCaptcha, katman olarak da Resim Tabanlı Captcha'nin tercih edildiği görülmektedir.

5.2.7. Kişisel siteler ve bloglar

Kişisel siteler ve bloglar siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen banka siteleri statüsüne sahip siteler baz alınarak gruba alınmıştır.

Çizelge 5.15. Kişisel siteler ve bloglar

	İncelenen Kişisel Siteler ve Bloglar	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Chip	Evet	reCaptcha	Resim Tabanlı
2	Schilda	Hayır	Yok	Yok
3	Journo	Hayır	Yok	Yok
4	Hizliadam.com	Evet	reCaptcha	Resim Tabanlı
5	Vpmavi.com	Evet	Matematik Capctha	Metin Tabanlı
6	jimithewkl	Hayır	Yok	Yok
7	Pinquitte	Hayır	Yok	Yok
8	homoeconomicus	Hayır	Yok	Yok
9	futurism	Hayır	Yok	Yok
10	adtorium	Evet	Basit Captcha	Metin Tabanlı

Çizelge 5.15. verileri incelendiğinde kişisel siteler ve bloglarda Captcha pek tercih edilmediği görülmektedir. Bunun sebebi olarak da kişisel site ve bloglarda daha çok herkese açık bilgi paylaşımı yapıldığı için denebilir.

5.2.8. Eğitim siteleri

Eğitim siteleri incelenirken; arama motorlarında tarama yapıldığında en çok tercih edilen eğitim siteleri statüsüne sahip web siteler baz alınarak incelemeye alınmıştır.

Okul siteleri

Okul siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen okul siteleri statüsüne sahip siteler baz alınarak gruba alınmıştır.

Çizelge 5.16. Okul siteleri

	İncelenen Okul Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Ted Ankara Koleji	Hayır	Yok	Yok
2	Ankara Fen	Evet	Karmaşık Captcha	Metin Tabanlı
3	Robert Koleji	Evet	Basit Captcha	Metin Tabanlı
4	Sınav Koleji	Evet	reCaptcha	Resim Tabanlı
5	Bahçeşehir	Evet	reCaptcha	Resim Tabanlı
6	İsmet İnönü İO	Evet	Matematik Captcha	Metin Tabanlı
7	Gazi Kolej	Hayır	Yok	Yok
8	Galatasaray Lisesi	Evet	reCaptcha	Resim Tabanlı
9	Açık Öğretim Lisesi	Evet	Matematik Captcha - Karmaşık Captcha	Metin Tabanlı
10	Ankara Anadolu Lisesi	Evet	Karmaşık Captcha	Metin Tabanlı
11	e-Okul	Evet	Basit Captcha	Metin Tabanlı
12	Mebsis	Evet	Basit Captcha	Metin Tabanlı

Çizelge 5.16. verileri incelendiğinde okul sitelerinde Captcha türü olarak daha çok reCaptha ve Matematik Captcha katman olarak da resim ve metin tabanlı Captcha'nin tercih edildiği görülmektedir. Çizelge 5.16. verileri yorumlandığında okul sitelerinde Captcha tercih edilmediği sitelerin de olduğu görülmektedir.

Üniversite siteleri

Üniversite siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen üniversite siteleri statüsüne sahip siteler baz alınarak gruba alınmıştır.

Çizelge 5.17. Üniversite siteleri

	İncelenen Üniversite Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Gazi Üniversitesi	Hayır	Yok	Yok
2	Tobb	Evet	Basit Captcha	Metin Tabanlı
3	Odtü	Evet	Karmaşık Captcha	Metin Tabanlı
4	Bilkent	Evet	reCaptcha	Resim Tabanlı
5	Hacettepe	Evet	reCaptcha	Resim Tabanlı
6	YüzüncüYıl	Evet	Basit Captcha	Metin Tabanlı
7	Erciyes	Evet	reCaptcha	Resim Tabanlı
8	Fırat	Evet	reCaptcha	Resim Tabanlı
9	DokuzEylül	Evet	reCaptcha	Resim Tabanlı
10	Hacı Bayram Veli Üniversitesi	Evet	reCaptcha	Resim Tabanlı
11	Galatasaray Üniversitesi	Evet	reCaptcha	Resim Tabanlı

Çizelge 5.17. verileri incelendiğinde üniversite sitelerinde Captcha türü olarak daha çok reCaptha, katman olarak da resim tabanlı Captcha (güvenlik godu)'nin tercih edildiği görülmektedir. Çizelge verileri yorumlandığında üniversite sitelerinde Captcha tercih edilmediği sitelerin de olduğu görülmektedir.

Dershane siteleri

Dershane siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen dershane siteleri statüsüne sahip siteler baz alınarak gruba alınmıştır.

Çizelge 5.18. Dershane siteleri

	İncelenen Dershane Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Akındil	Evet	Matematik Captcha	Metin Tabanlı
2	English Center	Evet	Matematik Captcha	Metin Tabanlı
3	Just English	Hayır	Yok	Yok
4	AmericanCulture	Hayır	Yok	Yok
5	Odtü Dershane	Hayır	Yok	Yok
6	Matematik Akademi	Hayır	Yok	Yok
7	Pegem	Hayır	Yok	Yok
8	Garanti Akademi	Hayır	Yok	Yok
9	Final Eğitim	Hayır	Yok	Yok
10	Perfect English	Evet	Matematik Captcha	Metin Tabanlı

Çizelge 5.18. verileri incelendiğinde dershane sitelerinde Captcha türü olarak daha çok matematik, katman olarak da metin tabanlı Captcha'nın tercih edildiği görülmektedir. Çizelge verileri yorumlandığında dershane sitelerinde Captcha pek tercih edilmediği görülmektedir.

Uzaktan eğitim siteleri

Uzaktan eğitim siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen uzaktan eğitim siteleri statüsüne sahip siteler baz alınarak gruba alınmıştır.

Çizelge 5.19. Uzaktan eğitim siteleri

	İncelenen Uzaktan Eğitim Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Akındil	Evet	Matematik Captcha	Metin Tabanlı
2	Udemy	Evet	reCaptcha	Resim Tabanlı
3	Ankara Dil	Hayır	Yok	Yok
4	AmericanCulture	Hayır	Yok	Yok
5	Cambly	Hayır	Yok	Yok
6	Rosettastone	Hayır	Yok	Yok
7	Ahmet Yesevi	Evet	Karmaşık Captcha	Metin Tabanlı
8	Canlı Eğitim	Hayır	Yok	Yok
9	English Center	Evet	Matematik Captcha	Metin Tabanlı
10	BreakingEnglish	Hayır	Yok	Yok
11	UzaktanEğitim.com	Evet	Basit Captcha	Metin Tabanlı
12	Ekolej.net	Evet	Karmaşık Captcha	Metin Tabanlı

Çizelge 5.19. verileri incelendiğinde uzaktan eğitim sitelerinde Captcha türü olarak daha çok matematik ve karmaşık, katman olarak da metin tabanlı Captcha'nin tercih edildiği görülmektedir. Çizelge verileri yorumlandığında uzaktan eğitim sitelerinde Captcha tercih edilmediği sitelerin de çokça olduğu görülmektedir.

Yayınevi siteleri

Yayınevi siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen yayınevi siteleri statüsüne sahip siteler baz alınarak gruba alınmıştır.

Çizelge 5.20. Yayınevi siteleri

	İncelenen Yayınevi Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Benim Hocam	Evet	Karmaşık Captcha	Metin Tabanlı
2	KitapYurdu	Evet	Karmaşık Captcha	Resim Tabanlı
3	Tudem	Evet	Karmaşık Captcha	Metin Tabanlı
4	İnkılap	Evet	Karmaşık Captcha	Metin Tabanlı
5	İletişim	Hayır	Yok	Yok
6	Can Çocuk	Hayır	Yok	Yok
7	Günüşiği	Hayır	Yok	Yok
8	Elma Yayınevi	Evet	Karmaşık Captcha	Metin Tabanlı
9	Türkiye İş Bankası Kültür Yayınları	Hayır	Yok	Yok
10	Pearson	Hayır	Yok	Yok

Çizelge 5.20. verileri incelendiğinde yayınevi sitelerinde Captcha türü olarak daha çok karmaşık, katman olarak da metin tabanlı Captcha 'nin tercih edildiği görülmektedir. Çizelge verileri yorumlandığında yayınevi sitelerinde Captcha tercih edilmediği sitelerin de olduğu görülmektedir.

5.2.9. Firma siteleri

Firma siteleri incelemeye alınırken; arama motorlarında tarama yapıldığında en çok tercih edilen firma siteleri statüsüne sahip web siteler baz alınarak incelemeye alınmıştır.

Çizelge 5.21. Firma siteleri

	İncelenen Firma Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Ford	Evet	reCaptcha	Resim Tabanlı
2	Petrol Ofisi	Evet	Basit Captcha	Metin Tabanlı
3	Tüpraş	Evet	reCaptcha	Resim Tabanlı
4	Bim	Evet	Basit Captcha	Metin Tabanlı
5	Migros	Evet	Karmaşık Captcha	Metin Tabanlı
6	Arçelik	Evet	reCaptcha	Resim Tabanlı
7	Türk Telekom	Evet	Karmaşık Captcha	Metin ve Ses Tabanlı
8	Coca Cola Türkiye	Evet	Karmaşık Captcha	Metin Tabanlı
9	Aselsan	Evet	Karmaşık Captcha	Metin Tabanlı
10	Microsoft	Evet	reCaptcha	Resim Tabanlı

Çizelge 5.21. verileri incelendiğinde firma sitelerinde Captcha türü olarak daha çok karmaşık ve reCaptcha, katman olarak da metin ve resim tabanlı Captcha'nin tercih edildiği görülmektedir. Çizelge verileri yorumlandığında firma sitelerinde Captcha genel olarak tercih edildiği görülmektedir.

5.2.10. Sağlık siteleri

Sağlık siteleri incelemeye alınırken; arama motorlarında tarama yapıldığında en çok tercih edilen sağlık siteleri statüsüne sahip web siteler baz alınarak incelemeye alınmıştır.

E-randevu siteleri

E-randevu (elektronik randevu) siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen e-randevu (elektronik randevu) siteleri statüsüne sahip siteler baz alınarak gruba alınmıştır.

Çizelge 5.22. E-randevu siteleri

	İncelenen Randevu Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	MHRS	Evet	reCaptcha	Resim Tabanlı
2	Lokman Hekim Randevu	Evet	Basit Captcha	Metin Tabanlı
3	Kolay Randevu	Evet	reCaptcha	Resim Tabanlı
4	Bülent Ecevit Hastanesi Randevu Sistemi	Hayır	Yok	Yok
5	Düzce Üniversite Hastanesi Randevu Sistemi	Hayır	Yok	Yok
6	Namık Kemal Üniversite Hastanesi Randevu Sistemi	Hayır	Yok	Yok
7	Maya Göz Randevu	Evet	Matematik Captcha	Metin Tabanlı
8	Gazi Üniversitesi Diş Hekimliği Randevu	Evet	Matematik Captcha	Metin Tabanlı
9	Dünya Göz	Evet	Karmaşık Captcha	Metin Tabanlı
10	Umay Güzellik	Hayır	Yok	Yok

Çizelge 5.22. verileri incelendiğinde e-randevu (elektronik randevu) sitelerinde Captcha türü olarak belirgin bir türün olmadığı ama katman olarak daha çok metin ve resim tabanlı Captcha'nın tercih edildiği görülmektedir. Çizelge verileri yorumlandığında yayınevi sitelerinde Captcha tercih edilmediği sitelerin de olduğu görülmektedir.

E-tahlil (elektronik tahlil) sonuç siteleri

E-tahlil (elektronik tahlil) sonuç siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen e-tahlil (elektronik tahlil) sonuç siteleri statüsüne sahip siteler baz alınarak gruba alınmıştır.

Çizelge 5.23. E-tahlil sonuç siteleri

	İncelenen E-Tahlil Sonuç Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	E-Nabız	Evet	reCaptcha	Resim Tabanlı
2	Lokman Hekim E-Tahlil	Evet	Basit Captcha	Metin Tabanlı
3	Ankara Halk Sağlığı Lab	Hayır	Yok	Yok
4	Pamukkale Üniversite Hastanesi Lab Sonuç	Evet	Matematik Captcha	Metin ve Ses Tabanlı
5	Ankara Bilgi Hastanesi Tahlil Sonuç	Evet	reCaptcha	Resim Tabanlı
6	KKTC Sağlık Bakanlığı	Evet	Basit Captcha	Resim Tabanlı
7	İzmir Tepecik Araştırma ve Eğitim Araştırma Hastanesi Tahlil Sonuç	Evet	Matematik Captcha	Metin ve Ses Tabanlı
8	Medical Park E-Sonuç	Hayır	Yok	Yok
9	Kent Sağlık Grubu	Hayır	Yok	Yok
10	Liv Hospital	Evet	reCaptcha	Resim Tabanlı

Çizelge 5.23. verileri incelendiğinde e-tahlil (elektronik tahlil) sonuç sitelerinde Captcha türü olarak daha çok reCaptcha, katman olarak da resim tabanlı Captcha'nın tercih edildiği görülmektedir. Çizelge verileri yorumlandığında e-tahlil (elektronik tahlil) sonuç sitelerinde Captcha tercih edilmediği sitelerin de olduğu görülmektedir. Ayrıca Matematik Captcha (güvenlik kodu kullanan sitelerin ses ve metin tabanlı katmanları birlikte kullandığı da görülmektedir.

Hastane siteleri

Hastane siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen hastane siteleri statüsüne sahip web siteler baz alınarak gruba alınmıştır.

Çizelge 5.24. Hastane siteleri

	İncelenen Hastane Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Acıbadem	Evet	Karmaşık Captcha	Metin Tabanlı
2	Amerikan Hastanesi	Evet	Karmaşık Captcha	Metin Tabanlı
3	Başkent	Evet	Karmaşık Captcha - Matematik Captcha	Metin Tabanlı
4	Yeditepe Üniversite Hastanesi	Hayır	Yok	Yok
5	Medical Park	Hayır	Yok	Yok
6	Memorial	Evet	Matematik Captcha - reCaptcha	Metin Tabanlı - Resim Tabanlı
7	Medicana	Hayır	Yok	Yok
8	Bayındır Sağlık Grubu	Hayır	Yok	Yok
9	Florence	Evet	reCaptcha	Resim Tabanlı
10	Medipol Sağlık Grubu	Evet	reCaptcha	Resim Tabanlı
11	Medipol Online	Evet	Karmaşık Captcha	Metin Tabanlı
12	Hacettepe	Evet	Basit Captcha	Metin Tabanlı

Çizelge 5.24. verileri incelendiğinde hastane sitelerinde Captcha türü olarak daha çok reCaptcha ve Karmaşık, katman olarak da resim ve metin tabanlı Captcha'nin tercih edildiği görülmektedir. Çizelge verileri yorumlandığında hastane sitelerinde Captcha tercih edilmediği sitelerin de olduğu görülmektedir. Ayrıca hastane sitelerin bazılarında hem reCaptcha hem de Matematik Captcha kullanıldığı görülmektedir.

Eczane siteleri

Eczane siteleri inceleme grubuna dahil edilirken, arama motorlarında tarama yapıldığında en çok tercih edilen eczane siteleri statüsüne sahip web siteler baz alınarak gruba alınmıştır.

Çizelge 5.25. Eczane siteleri

	İncelenen Eczane Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Eczane.com	Evet	Karmaşık Captcha	Resim Tabanlı
2	WebEczanem	Evet	reCaptcha	Resim Tabanlı
3	Turuncu Eczane	Evet	Basit Captcha	Resim Tabanlı
4	Eczane Online	Evet	Basit Captcha	Metin Tabanlı
5	Nar Eczanesi	Evet	Basit Captcha	Resim Tabanlı
6	Dermo Eczanem	Evet	Basit Captcha	Resim Tabanlı
7	Recete.com	Evet	Matematik Captcha	Metin Tabanlı
8	Dermo Kozmetik	Evet	Karmaşık Captcha	Resim Tabanlı
9	Farmasi	Evet	Karmaşık Captcha	Resim Tabanlı
10	KırmızıBeyaz	Evet	Basit Captcha	Metin Tabanlı

Çizelge 5.25. verileri incelendiğinde eczane sitelerinde Captcha türü olarak daha çok basit, katman olarak da metin tabanlı Captcha'nin tercih edildiği görülmektedir. Çizelge verileri yorumlandığında eczane sitelerinde Captcha türünden en az birinin genellikle tercih edildiği görülmektedir.

5.2.11. Kamu kurumu siteleri

Kamu kurum web siteleri inceleme grubuna dahil edilirken; arama motorlarında tarama yapıldığında en çok tercih edilen kamu kurumu siteleri statüsüne sahip web siteler baz alınarak incelemeye alınmıştır.

Çizelge 5.26. Kamu kurum siteleri

	İncelenen Kamu Kurumu Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	TBMM	Hayır	Yok	Yok
2	Adalet Bakanlığı	Evet	reCaptcha	Resim Tabanlı
3	YÖK	Evet	reCaptcha	Resim Tabanlı
4	Atom Enerji Kurumu	Evet	reCaptcha	Resim Tabanlı
5	TÜBİTAK	Evet	Karmaşık Captcha	Metin Tabanlı - Resim Tabanlı
6	İŞKUR	Evet	Matematik Captcha	Metin Tabanlı
7	TRT	Evet	Matematik Captcha	Resim Tabanlı
8	Devlet Personel Başkanlığı	Evet	Matematik Captcha	Metin Tabanlı
9	EGM	Evet	Basit Captcha	Metin Tabanlı
10	MEB	Evet	Matematik Captcha	Metin Tabanlı
11	Sağlık Bakanlığı	Evet	reCaptcha	Resim Tabanlı
12	Merkez Bankası	Evet	Basit Captcha	Metin Tabanlı
13	BTK	Evet	reCaptcha	Resim Tabanlı
14	Cumhurbaşkanlığı	Evet	reCaptcha	Resim Tabanlı
15	Sanayi ve Teknoloji Bakanlığı	Evet	Matematik Captcha	Resim Tabanlı

Çizelge 5.26. verileri incelendiğinde kamu kurum sitelerinde Captcha türü olarak daha çok reCaptcha, katman olarak da resim tabanlı Captcha'nin tercih edildiği görülmektedir.

Çizelge verileri yorumlandığında kamu kurum sitelerinde Captcha türünden en az birinin genellikle tercih edildiği görülmektedir. Yapılan inceleme sonucunda kamu kurum sitelerin çoğunda E-Devlet Bilgi Kapısı üzerinden erişim sağlandığı için E-devlet (elektronik devlet) üzerinden reCaptcha kullanımı tercih edilmektedir.

5.2.12. Anket siteleri

Anket web siteleri inceleme grubuna dahil edilirken; arama motorlarında tarama yapıldığında en çok tercih edilen anket siteleri statüsüne sahip web siteler baz alınarak incelemeye alınmıştır.

Çizelge 5.27. Anket siteleri

	İncelenen Anket Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	valuedopinions.com	Evet	reCaptcha	Resim Tabanlı
2	napolyon.com	Evet	reCaptcha - Resim Captcha	Resim Tabanlı
3	Acop.com	Evet	reCaptcha	Resim Tabanlı
4	Toluna.com	Evet	reCaptcha	Resim Tabanlı
5	Myiyo.com	Evet	reCaptcha	Resim Tabanlı
6	Napolyon.com	Evet	reCaptcha	Resim Tabanlı
7	Benderimki.com	Evet	reCaptcha	Resim Tabanlı
8	Ipsos.com	Evet	Basit Captcha	Metin Tabanlı
9	Globaltestmarket.com	Evet	reCaptcha	Resim Tabanlı
10	Marketagent.com	Evet	reCaptcha	Resim Tabanlı
11	Benderimki.com	Evet	reCaptcha	Resim Tabanlı
12	Expower.net	Hayır	Yok	Yok

Çizelge 5.27. verileri incelendiğinde anket sitelerinde Captcha türü olarak daha çok reCaptcha, katman olarak da resim tabanlı Captcha'nın tercih edildiği görülmektedir. Çizelge verileri yorumlandığında anket sitelerinde Captcha türünden en az birinin genellikle tercih edildiği görülmektedir. Sağlıklı anket istatistikleri oluşturmak için Captcha ya da benzeri güvenlik yöntemlerin uygulanması gerekmektedir.

5.2.13. Eğlence siteleri

Eğlence web siteleri inceleme grubuna dahil edilirken; arama motorlarında tarama yapıldığında en çok tercih edilen eğlence siteleri statüsüne sahip web siteler baz alınarak incelemeye alınmıştır.

Oyun siteleri

Oyun web siteleri inceleme grubuna dahil edilirken; arama motorlarında tarama yapıldığında en çok tercih edilen oyun siteleri statüsüne sahip web siteler baz alınarak gruba alınmıştır.

Çizelge 5.28. Oyun siteleri

	İncelenen Oyun Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Miniclip.com	Evet	reCaptcha	Resim Tabanlı
2	MetalUp	Evet	reCaptcha	Resim Tabanlı
3	Playretrogames.com	Evet	Basit Captcha	Metin Tabanlı
4	Oyun Gemisi	Hayır	Yok	Yok
5	Cocux.com	Hayır	Yok	Yok
6	Pogo.com	Evet	Basit Captcha	Metin Tabanlı
7	Çarpım Çizelgesu	Hayır	Yok	Yok
8	mmogames.com	Hayır	Yok	Yok
9	Oyun Skor	Evet	reCaptcha	Resim Tabanlı
10	Zeka ve akıl oyunları	Evet	Basit Captcha	Resim Tabanlı

Çizelge 5.28. verileri incelendiğinde oyun sitelerinde Captcha türü olarak daha çok reCaptcha ve basit, katman olarak da resim ve metin tabanlı Captcha'nin tercih edildiği görülmektedir. Çizelge verileri yorumlandığında oyun sitelerinde Captcha tercih edilmediği sitelerin de görülmektedir.

Bahis siteleri

Bahis web siteleri inceleme grubuna dahil edilirken; arama motorlarında tarama yapıldığında en çok tercih edilen bahis siteleri statüsüne sahip web siteler baz alınarak gruba alınmıştır.

Çizelge 5.29. Bahis siteleri

	İncelenen Bahis Siteleri	Captcha Kullanılm ış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Nesine.com	Evet	Karmaşık Captcha	Metin Tabanlı
2	Bilyoner.com	Evet	reCaptcha	Resim Tabanlı
3	tipobet0906.c om	Evet	reCaptcha	Resim Tabanlı
4	gobahis53.co m	Hayır	Yok	Yok
5	dumanbet20. com	Evet	Basit Captcha	Metin Tabanlı
6	sekabet330.c om	Evet	Basit Captcha	Metin Tabanlı
7	bahsegel19.c om	Hayır	Yok	Yok
8	perabet191.c om	Evet	Basit Captcha	Metin Tabanlı
9	nakitbahis71. com	Hayır	Yok	Yok
10	mobilbahis15 4.com	Hayır	Yok	Yok

Çizelge 5.29. verileri incelendiğinde bahis sitelerinde Captcha türü olarak daha çok reCaptcha ve basit, katman olarak da resim ve metin tabanlı Captcha'nın tercih edildiği görülmektedir. Çizelge verileri yorumlandığında bahis sitelerinde Captcha tercih edilmediği sitelerinde görülmektedir.

Gezi siteleri

Gezi web siteleri inceleme grubuna dahil edilirken; arama motorlarında tarama yapıldığında en çok tercih edilen gezi web siteleri statüsüne sahip web siteler baz alınarak gruba alınmıştır.

Çizelge 5.30. Gezi siteleri

	İncelenen Gezi Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Gezimanya.com	Evet	reCaptcha	Resim Tabanlı
2	Gezikumbarasi.com	Hayır	Yok	Yok
3	Pratik Gezi Rehberi	Hayır	Yok	Yok
4	Kendingez.com	Hayır	Yok	Yok
5	Keşfet.com	Hayır	Yok	Yok
6	gezialemi	Evet	Matematik Captcha	Metin Tabanlı
7	themagger	Hayır	Yok	Yok
8	gezi-yorum	Evet	reCaptcha	Resim Tabanlı
9	Yoldaolmak.com	Hayır	Yok	Yok
10	Sirtcantalılar.com	Hayır	Yok	Yok

Çizelge 5.30. verileri incelendiğinde gezi sitelerinde Captcha (güvenlik kodu pek tercih edilmediği bunun sebebi olarak da gezi sitelerin daha çok bilgilendirme amaçlı olmasındandır. Gezi sitelerde işlemi gerektiren durumlarda da Captcha türü olarak daha çok reCaptcha, katman olarak da resim tabanlı Captcha'nin tercih edildiği görülmektedir.

5.2.14. Sanatsal siteler

Sanatsal web siteleri incelemeye dahil edilirken; arama motorlarında tarama yapıldığında en çok tercih edilen sanatsal siteleri statüsüne sahip web siteler baz alınarak incelemeye alınmıştır.

Çizelge 5.31. Sanatsal siteleri

	İncelenen Sanatsal Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Sanatlog.net	Hayır	Yok	Yok
2	Egoistokur.net	Hayır	Yok	Yok
3	Dunyabizim.net	Evet	Matematik Captcha	Metin Tabanlı
4	Futuristika.net	Hayır	Yok	Yok
5	Murekkephaber.net	Evet	reCaptcha	Resim Tabanlı
6	Sosyolojisi.net	Hayır	Yok	Yok
7	Etilen.net	Evet	Matematik Captcha	Metin Tabanlı
8	Zuhurat.net	Hayır	Yok	Yok
9	Nouvart.net	Hayır	Yok	Yok
10	Kayiprihtim.com	Hayır	Yok	Yok

Çizelge 5.31 verileri incelendiğinde sanatsal sitelerinde Captcha pek tercih edilmediği bunun sebebi olarak da sanatsal sitelerin daha çok bilgilendirme amaçlı olmasındandır. Sanatsal sitelerde işlem gerektiren durumlarda da Captcha türü olarak daha çok matematik, katman olarak da metin tabanlı Captcha'nin tercih edildiği görülmektedir.

5.2.15. Portal siteleri

Portal web siteleri inceleme grubuna dahil edilirken; arama motorlarında tarama yapıldığında en çok tercih edilen portal siteleri statüsüne sahip siteler baz alınarak incelemeye alınmıştır.

Çizelge 5.32. Portal siteleri

	İncelenen Portal Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Msn	Evet	reCaptcha	Resim Tabanlı
2	turkish-media	Evet	reCaptcha	Resim Tabanlı
3	yahoo	Evet	Güncel Captcha	Metin Tabanlı
4	ucuzproje	Evet	reCaptcha	Resim Tabanlı
5	mynet	Evet	Karmaşık Captcha	Resim Tabanlı
6	google	Evet	reCaptcha	Resim Tabanlı
7	bing	Evet	Güncel Captcha	Metin Tabanlı
8	QQ.com	Evet	Slider Captcha	Metin Tabanlı
9	Reddit.com	Evet	reCaptcha	Resim Tabanlı
10	yandex	Evet	Güncel Captcha	Metin Tabanlı

Çizelge 5.32. verileri incelendiğinde portal sitelerinde Captcha türü olarak reCaptcha, katman olarak da resim tabanlı Captcha tercih edildiği görülmektedir. Çizelge verileri yorumlandığında portal sitelerinde Captcha kullanımının yaygın olduğu en az bir modelin tercih edildiği sonucuna varabiliriz.

5.2.16. E-posta servis sağlayıcı siteleri

E-posta (elektronik posta) servis sağlayıcı siteler araştırma grubuna dahil edilirken; arama motorlarında tarama yapıldığında en çok tercih edilen e-posta (elektronik posta) servis sağlayıcı siteleri statüsüne sahip web siteler baz alınarak incelemeye alınmıştır.

Çizelge 5.33. E-posta servis sağlayıcı siteleri

	İncelenen E-Posta Servis Sağlayıcı Siteleri	Captcha Kullanılmış Mı?	Kullanılan Captcha Türü	Kullanılan Captcha Katmanı
1	Gmail	Evet	reCaptcha	Resim Tabanlı
2	outlook	Evet	reCaptcha	Resim Tabanlı
3	Yandexmail	Evet	reCaptcha	Resim Tabanlı
4	icloud	Evet	Karmaşık Captcha	Resimve Ses Tabanlı
5	Yahoo mail	Evet	reCaptcha	Resim Tabanlı
6	Protonmail	Hayır	Yok	Yok
7	zoho	Evet	Karmaşık Captcha	Metin Tabanlı
8	Aol Mail	Evet	reCaptcha	Resim Tabanlı
9	My Way Mail	Evet	reCaptcha	Resim Tabanlı
10	GMX	Evet	reCaptcha	Resim Tabanlı

Çizelge 5.33. verileri incelendiğinde e-posta servis sağlayıcı sitelerinde Captcha türü olarak reCaptcha, katman olarak da resim tabanlı Captcha tercih edildiği görülmektedir. Çizelge verileri yorumlandığında portal sitelerinde çoğunlukla bir Captcha modelin kullanıldığı görülmektedir.

5.3. İncelenen Web Sitelerinde Captcha Genel Kullanımı

Çizelge 5.34. Captcha kullanım durumu

İncelenen Captcha Sayısı	Captcha Kullanım Sayısı	Captcha Kullanmayan Sayısı
340	236	104

Web sitelerinde Captcha kullanım durumuna göre bölüm 5.2.'den analiz edilerek oluşturulan 5.34.'deki Çizelge incelendiğinde; toplamda incelenen 340 web sitesinden 236 sitede Captcha kullanılırken, 104 tanesinde kullanılmadığı görülmektedir. Captcha kullanmayan sitelerin siber saldırı tehditlerine daha açık olduğu yorumu yapılabilir.

5.4. Web Sitelerinde Captcha Türü Kullanım Durum İncelenmesi

Çizelge 5.35. Captcha çeşitliliğinde kullanım

Captcha Türü	Kullanım Sayısı (f)
Basit Captcha	39
Güncel Captcha	14
Matematik Captcha	24
Karmaşık Captcha	35
Nesneli Captcha	-
Resim Captcha	4
Slider Captcha	5
reCaptcha	111
reCaptcha+MatematikCaptcha	1
reCaptcha+ KarmaşıkCaptcha	1
reCaptcha+Resim Captcha	1
MatematikCaptcha + KarmaşıkCaptcha	1
Toplam	236

Web sitelerinde Güvenlik Kodların (captcha) kullanım çeşitliliğine göre bölüm 5.2.'den analiz edilerek oluşturulan 5.35.'teki Çizelge incelendiğinde; Captcha kullanan incelenen 236 sitede açık ara fark ile en çok tercih edilen Captcha türüdür. Bunun tercih edilmediği yerlerde daha çok Basit ve Karmaşık Captcha olduğu görülmektedir. Nesneli Captcha hiç tercih edilmedi Çizelgeden görülmektedir. Çizelgedeki verilere göre en güncel Captcha olan reCaptcha'nın en tercih edilen olduğu sonucuna varırız.

5.5. Web Site Amacına Göre Captcha Katman İncelenmesi

Çizelge 5.36. Captcha kullanım amacına göre çeşitliliği

Kullanım Amacı	İncelenen Site Sayısı	Resim Katmanı Kullanım Sayısı (f)	Metin Katmanı Kullanım Sayısı (f)	Ses + Resim Katmanı Kullanım Sayısı (f)	Resim+Metin Katmanı Kullanım Sayısı (f)	Ses+Metin Katmanı Kullanım Sayısı (f)	Captcha(güvenlik kodu) Kullanmayan Sayısı (f)
Arama Motorları	15	1	7	-	-	-	7
Sosyal Medya Siteleri	21	16	5	-	-	-	2
Haber Siteleri	30	16	6	-	-	-	8
E-Ticaret Siteleri	30	8	7	-	-	-	15
İlan Siteleri	10	3	4	-	1	-	2
Finansal Kurum Siteleri	30	12	4	2	-	5	7
Kişisel Siteler ve Bloglar	10	2	2	-	-	-	6
Eğitim Siteleri	55	22	12	-	-	-	21
Firma Siteleri	10	4	5	-	-	1	0
Sağlık Siteleri	42	14	13	-	2	2	11
Kamu Kurum Siteleri	15	8	5	-	1	-	1
Anket Siteleri	12	10	1	-	-	-	1
Eğlence Siteleri	30	9	6	-	-	-	15
Sanatsal Siteler	10	1	2	-	-	-	7
Portal Siteleri	10	6	4	-	-	-	0
E-Posta Servis Sağlayıcı Siteler	10	7	1	1	-	-	1
Toplam	340	111	84	3	4	8	104

Web sitelerin kullanım amaçlarına göre kullanılan Captcha katmanı bölüm 5.2.'den analiz edilerek oluşturulan Çizelge 5.36.'daki Çizelge incelendiğinde; Captcha katmanı olarak incelenen 236 sitede açık ara fark ile en çok tercih edilen Resim Tabanlı Captcha katmanıdır. Bunun tercih edilmediği durumlarda daha çok Metin Tabanlı Captcha katmanının tercih edildiği görülmektedir. En az tercih edilen katmanlar ise Ses + Resim ve Resim + Metin kombinasyonundan oluşan yapılar olduğu görülmektedir.

5.6. Web Site Amacına Göre Captcha Kullanım İstatistiği

Çizelge 5.37. Amaca göre captcha kullanımı

Kullanım Amacı	İncelenen Site Sayısı (f)	Captcha Kullanım Sayısı (f)	Captcha Kullanmayan Sayısı (f)	Yüzde Kullanım (%)
Arama Motorları	15	8	7	%53,33
Sosyal Medya Siteleri	21	19	2	%90,4
Haber Siteleri	30	22	8	%73,33
E-Ticaret Siteleri	30	15	15	%50
İlan Siteleri	10	8	2	%80
Finansal Kurum Siteleri	30	23	7	%76,66
Kişisel Siteler ve Bloglar	10	4	6	%40
Eğitim Siteleri	55	34	21	%61,81
Firma Siteleri	10	10	0	%100
Sağlık Siteleri	42	31	11	%73,8
Kamu Kurum Siteleri	15	14	1	%93,33
Anket Siteleri	12	11	1	%91,66
Eğlence Siteleri	30	15	15	%50
Sanatsal Siteler	10	3	7	%30
Portal Siteleri	10	10	0	%100
E-Posta Servis Sağlayıcı Siteler	10	9	1	%90
Toplam	340	236	104	%69,41

Web site amacına göre captchaların kullanım durumu incelendiğinde bölüm 5.2’den analiz edilerek Çizelge 5.37.’deki Çizelgede istatistik olarak verilmiştir. Çizelgede görüldüğü gibi Captcha kullanım en çok tercih eden gruplar %100 kullanım ile portal ve firma siteleri olduğu görülmektedir. %90 ve üstü kullanım ile e-posta servis sağlayıcı, anket ve sosyal

medya siteleri olduğu görülmektedir. En az tercih eden siteler ise %30 kullanım ile sanatsal ve e-ticaret siteleri olduğu görülmektedir.

5.7. Web Site Amacına En Uygun Kural Tabanlı Captcha Algoritması Oluşturma

Kural tabanlı mantık çerçevesinde 5.1'deki Çizelge sonuçları yorumlandığında 5.7.1 ve 5.7.2'deki çıkarım Çizelgeleri oluşturulmuştur.

Çizelge 5.38. Captcha katmanlarında güvenlik düzeyi

Captcha Katmanı	Güvenlik Düzeyi	Kural Taban Seviyesi
Metin Tabanlı	Çok Düşük	1
Resim Tabanlı	Orta	3
Ses Tabanlı	Düşük	2

Captcha katmanlarının kırılma seviyelerine göre kural tabanlı değerlendirilmesi yapıldığında 1 (tamamen güvenilir) ve 0 (tamamen güvensiz) aralığında 3 tane seçilebilir kural taban seviyesi Çizelge 5.38.'de oluşturulmuştur.

Çizelge 5.39. Captcha çeşitlerinde güvenlik düzeyi

Captcha Katmanı	Güvenlik Düzeyi	Kural Tabanlı Seviye
Basit Captcha	Çok Düşük	1
Güncel Captcha	Düşük	2
Matematik Captcha	Çok Düşük	1
Karmaşık Captcha	Orta	3
Nesneli Captcha	Orta	3
Resim Captcha	Yüksek	4
Slider Captcha	Yüksek	4
reCaptcha	Çok Yüksek	5

Captcha çeşitlerinin kırılma seviyelerine göre kural tabanlı olarak değerlendirilmesi yapıldığında 1 (tamamen güvenilir) ve 0 (tamamen güvensiz) aralığında 5 tane seçilebilir kural tabanlı seviye Çizelge 5.39.'da oluşturulmuştur.

Kural tabanı (rule base logic) çerçevesinde bölüm 5.4., 5.5. ve 5.6.'daki Çizelge sonuçları yorumlandığında 5.40., 5.41. ve 5.42.'deki çıkarım Çizelgeleri oluşturulmuştur.

Çizelge 5.40. Captcha katmanlarında kullanım sıklığı

Captcha Katmanı	Kullanım Sıklığı	Kural Tabanlı Seviyesi
Metin Tabanlı	111	3
Resim Tabanlı	84	2
Ses Tabanlı	11	1

Captcha katmanlarının kullanım sıklığına göre yani popülerliğine göre kural tabanı değerlendirilmesi yapıldığında 1 (çok popüler) ve 0 (popülerliği yok) aralığında 3 tane seçilebilir kural tabanı seviyesi Çizelge 5.40.'da oluşturulmuştur.

Çizelge 5.41. Captcha çeşitlerinde kullanım sıklığı

Captcha Katmanı	Kullanım Sıklığı	Kural Tabanı Seviye
Basit Captcha	39	6
Güncel Captcha	14	3
Matematik Captcha	24	4
Karmaşık Captcha	35	5
Nesneli Captcha	0	0
Resim Captcha	4	1
Slider Captcha	5	2
reCaptcha	111	7

Captcha çeşitlerimin kullanım sıklığına göre yani popülerliğine göre kural tabanı değerlendirilmesi yapıldığında 1 (çok popüler) ve 0 (popülerliği yok) aralığında 8 tane seçilebilir kural tabanı seviyesi Çizelge 5.41.'de oluşturulmuştur. Nesneli Captcha hiç kullanılmadığı için 0 seviyesi verilmiştir.

Çizelge 5.42. Site amacına göre captcha kullanım sıklığı

Kullanım Amacı	En Çok Kullanılan Captcha Katmanı	En Çok Kullanılan Captcha Türü	Kural Tabanı Seviye
Arama Motorları	Metin Tabanlı	Güncel Captcha	1, 3
Sosyal Medya Siteleri	Resim Tabanlı	reCaptcha	2, 7
Haber Siteleri	Resim Tabanlı	reCaptcha	2, 7
E-Ticaret Siteleri	Resim Tabanlı	reCaptcha	2, 7
İlan Siteleri	Metin Tabanlı	reCaptcha	1, 7
Finansal Kurum Siteleri	Resim Tabanlı	reCaptcha	2, 7
Kişisel Siteler ve Bloglar	Resim ve Metin Tabanlı	reCaptcha	1 ve 2, 7
Eğitim Siteleri	Resim Tabanlı	reCaptcha	2, 7
Firma Siteleri	Metin Tabanlı	reCaptcha ve Karmaşık Captcha	1, 7 ve 5
Sağlık Siteleri	Resim Tabanlı	reCaptcha ve Karmaşık Captcha	2, 7 ve 5
Kamu Kurum Siteleri	Resim Tabanlı	reCaptcha	2, 7
Anket Siteleri	Resim Tabanlı	reCaptcha	2, 7
Eğlence Siteleri	Resim Tabanlı	reCaptcha	2, 7
Sanatsal Siteler	Metin Tabanlı	Matematik	1, 4
Portal Siteleri	Resim Tabanlı	Güncel Captcha	2, 3
E-Posta Servis Sağlayıcı Siteler	Resim Tabanlı	reCaptcha	2, 7

Sitelerin kullanım amaçlarına göre ele alınan 400 sitenin 340 incelenmiştir. Bu kapsamda; kullanılan Captcha türü ve katmanları ele alığında her grup için en çok tercih edilenler Çizelge 5.42.'te verilmiştir. Bu Çizelge oluşturulurken bölüm 5.5 ve 5.6'daki çizelgelerden yararlanılmıştır. Kural tabanı seviyeleri ise Çizelge 5.41. ve 5.42.'den yararlanılarak oluşturulmuştur. Elde edilen veri ile kullanım amacına göre en popüler Captcha seçimi sağlanmaktadır.





6. SONUÇ VE ÖNERİLER

Bu bölümde elde edilen bulguların araştırılması ve incelenmesiyle; ortaya konan değerlere bağlı olarak ulaşılan sonuçlara ve bu sonuçlara dayalı olarak sunulan önerilere yer verilmektedir.

Bu araştırmada; temel problem çerçevesinde test edilen ana amaç ve alt amaçlara dayalı olarak şu sonuçlara varılmıştır;

1. Captcha katmanları literatür taraması ile toplanan verilere göre siber saldırılara karşı koyma ve kırılma oranları incelendiğinde, en güvenilir katmanın resim tabanlı olduğu, saldırılara en az direnen ise metin tabanlı olduğu sonucuna varılmıştır.
2. Captcha modelleri literatür taraması ile toplanan verilere göre siber saldırılara karşı koyma ve kırılma oranları incelendiğinde, en güvenilir modelin reCaptcha olduğu, saldırılara en az direnen modeller ise Basit ve Matematik modellerin olduğu tespit edilmiştir.
3. Web site geliştiricilerin sitelerinde Captcha kullanırken kullanacakları en güvenli katman ve modelin, Resim tabanlı reCaptcha olduğu sonucuna varılmıştır.
4. Bulguların elde edilmesi ve analiz edilmesi sonucunda Türkiye’de kullanılan 340 web sitenin 236 tanesinde Captcha kullanırken yüzde frekans olarak hesaplandığında %69,41; 104 tane web sitesinde ise Captcha kullanılmadığı yüzde frekans olarak hesaplandığında %30,58 oranında olduğu tespit edilmiştir.
5. Captcha kullanmayan 104 web sitesi incelendiğinde çoğunluğunun herkese açık (Public website) bilgi paylaşımı yapan blog, gezi, eğlence vb. olduğu sonucuna varılmıştır.
6. Captcha kullanmayan siteler ya başka güvenlik yöntemi almışlardır ya da tamamen dış siber saldırılara açık durumda olduğu tespit edilmiştir. Captcha kullanmayanlar daha çok gsm kod, mail doğrulama, hesap bağlama, hesap bloke etme, hesap kitleme, arka planda IP kontrol vb. önlemler aldığı tespit edilmiştir.

7. Captcha kullanan 236 web sitesi kullanılan Captcha katmanı bakımından analiz edildiğinde en çok tercih dilen katmanın %47,01 ile Resim tabanlı olduğu görülmüştür.
8. Captcha kullanan 236 web sitesi kullanılan Captcha modeli bakımından analiz edildiğinde en çok tercih dilen modellerin %47,01 ile reCaptcha, %16,52 ile Basit Captcha, %14,83 ile de Karmaşık Captchanın tercih edildiği ve %0,00 oranında Nesneli Captcha kullanıldığı tespit edilmiştir.
9. İncelenen 340 web sitesi kullanım amacına göre 16 grup olarak incelenip analizi sonucunda: Portal siteleri ve Firma sitelerin %100, Kamu Kurum siteleri %93,33, Anket siteleri %91,66, Sosyal Medya siteleri %90,4, E-posta Servis Sağlayıcı siteler %90, İlan siteleri %80, Finansal Kurum siteleri %76,66, Sağlık siteleri %73,8, Haber siteleri %73,33, Eğitim siteleri %61,81, Arama motorları %53,33, E-ticaret ve Eğlence siteleri %50, Kişisel Siteler ve Bloglar %40 ve Sanatsal siteler de %30 oranında bir Captcha modeli tercih ettiği sonucuna varılmıştır.
10. Yukarda belirtilen sonuçlar çerçevesinde ve elde edilen verilerle kural tabanı (rule base logic) tabanlı; güvenlik, popülerlik ve site amacı kriterlerine dayanan bir algoritma oluşturulmuştur. Algoritma web geliştiricilerin isteği doğrultusunda en güvenli, en popüler ve amaca en uygun Captcha Model ve Katmanı sunmaktadır.

Bu araştırmada elde edilen sonuçlara dayalı olarak; Captcha uygulamaları ve Captcha konusunda yapılması gereken araştırmalarla ilgili olarak aşağıdaki öneriler geliştirilmiştir;

1. Teknolojideki baş döndüren hızlı gelişmelerine paralel olarak sanal dünyada siber savaş da orantılı olarak artmaktadır. Bu kapsamda teknolojinin pozitif ve negatif yönlerinin eş zamanlı gelişme göstermesi sanal dünyada kullanıcıların daha rahat ve güvenli dolaşabilmeleri için çeşitli güvenlik önemleri alınmıştır. Bunlardan en temel olanı Captcha sistemleridir. Bu bakımdan geliştirilecek her web sitesinde Captcha kullanılması ya da türevi bir güvenlik uygulamasının kullanılması sağlanmalıdır.
2. Captcha kullanılması ehemmiyet taşıdığı gibi kullanılacak Captcha türü veya katmanın da bot saldırılar (kötücül siber saldırılar) tarafından aşılmamış yani kırılmamış olmasına dikkat edilmelidir.

3. Captcha kullanılmasının en efektif ve etkili bir şekilde iş görebilmesi için web sitelerin kullanım amaçlarına göre Captcha türünün ve katmanın tercih edilmesi hususu dikkate alınmalıdır.
4. Web site ziyaretçilerini bunaltmadan hizmet sunmak için kullanıcıyı zorlayıcı Captcha kullanılması yerine seviyeden seviyeye zorlaşan Captcha tercih edilmesi özendirilmelidir.
5. Captcha uygulamalarının yetersiz kaldığı durumlarda evrimleşmesi sonucu ortaya daha zor aşılabilecek basit yöntemlerden ziyade daha çok özel yapay zekâ örnekleriyle ihmal edilebilecek sistemler çıkmaktadır ve de bu zorlukta yapıların öğrenebilen yapay zekâ ile çözülebilmesi olayı Captcha doğrulama sahnesinden daha farklı bir boyuta taşımaktadır. Captcha'yı bu tarz yapay sinir ağları ile geliştirme yapan kişiler için de günden güne gelişen ve zorlaşan iyi bir test aracı olduğu ortadadır. Bu kapsamda; yapay zekâ teknikleri ile kullanıcıyı bunaltmayan gizli Captcha en güncel türü olan reCaptcha tercih edilmelidir.
6. Yeni araştırmalarda yeni bir Captcha modeli oluşturulurken, güncel teknolojiye ile yapay zekâ teknikleri kullanılması gerekmektedir. Bu minvalde kullanıcının web site geçinimlerinden, oturum bilgilerinden, erişim bilgilerinden faydalanarak daha da güvenli ve kullanıcı dostu sistemlere odaklı yapılması sağlanmalıdır.



KAYNAKLAR

- Çakır, H. ve Ulubatun, (2018). *Güvenlik Kodu Çeşitliliği ile Siber Tehditlere Karşı Güçlü güvenliğin sağlanması*, International of Human Sciences Journal ISSN:2458-9489 Volume 15 Issue 3
- Ulubatun, N., Yalçın, Nursel ve Alver, S., (2018). “*Diyabetik Retinopati Hastalığının Erken Tespiti İçin Derin Öğrenme ile Retina Görüntülerin Sınıflandırılması*” 26th Signal Processing and Communications Applications Conference (SIU) Publisher:IEEE
- Gao, H., Tang, M., Liu, Y., Zhang, P. ve Liu, X. (2017), *Research on the Security of Microsoft’s Two-layer Captcha* IEEE Transactions on Information Forensics and Security, IEEE Transactions on Information Forensics and Security (Volume: 12 , Issue: 7 , July 2017)
- Von Ahn, L., Blum, M., Hopper, N. J. and Langford, J., *Captcha: Using hard ai problems for security*, in Advances in Cryptology EUROCRYPT 2003. Springer, 2003, pp. 294–311.
- Altaş, İ. H., (1999) *Bulanık Mantık: Bulanıklık Kavramı* Enerji, Elektrik, Elektromekanik-3e, Temmuz 1999, Sayı 62, Sayfalar:80-85, Bilesim yayıncılık A.Ş., İstanbul
- Alıcı, M. ve Karatepe, E. (Yazarlar). (2002). *Bulanık Mantık ve Matlab Uygulamaları*, İzmir: Engin Kitapevi Yayınları, 102-105.
- Von Ahn, L. , Blum, M. . Hopper, N. J and Langford, J. *Telling humans and computers apart automatically*, Communications of the ACM, vol. 47, no. 2, pp. 56–60, 2004.
- Bursztein, E., Martin, M. and Mitchell, J. *Text-based captcha strengths and weaknesses*, in Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011, pp. 125–138.
- Yan, J. and Ahmad, El A. S. *Usability of captchas or usability issues in captcha design*, in Proceedings of the 4th symposium on Usable privacy and security. ACM, 2008, pp. 44–52.
- Chellapilla, K., Larson, K., Simard, P. Y. and Czerwinski, M. *Building segmentation based human-friendly human interaction proofs (hips)*, in Human Interactive Proofs. Springer, 2005, pp. 1–26.
- C. Kumar, L. Kevin, S. Patrice, Y., and C. Mary, *Computers beat humans at single character recognition in reading based human interaction proofs (hips)*, in CEAS 2005- Second Conference on Email and Anti-Spam, July 21-22, 2005, Stanford University, California, USA, 2005.
- Yan, J. and El Ahmad, A. S. *Breaking visual captchas with naive pattern recognition algorithms*, in Computer Security Applications, Conference, 2007. ACSAC 2007. Twenty-Third Annual. IEEE, 2007, pp. 279–291.

Yan, J. and El Ahmad, A. S. *A low-cost attack on a Microsoft captcha*, in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 543–554.

McDermott, D. (2014), On the Claim that a Look-Up Table Program could Pass the Turing Test, *Minds and Machines*, 24: 143–88.

McDermott, D. (2014), *On the Claim that a Look-Up Table Program could Pass the Turing Test*, *Minds and Machines*, 24: 143–88.

Ahn, L., Blum, M., Nicholas, J. H. and Langford, J. *CAPTCHA: Using Hard AI Problems For Security* Yorktown Heights NY 10598, USA

İnternet: Yahoo Captcha Hacked *Cipec*.URL: <http://it.slashdot.org/story/08/01/30/0037254/yahoo-captcha-hacked>, Son Erişim Tarihi: 17.03.2018.

İnternet: Audio Security System Cracked *Cipec*.URL: <http://www.technologyreview.com/computing/37690/?mod=related>, Son Erişim Tarihi: 11.05.2019.

İnternet: Image Security Captchas Hacked *Cipec*.URL: <http://www.technologyreview.com/web/21519/page1/>, Son Erişim Tarihi: 11.05.2019.

İnternet: New Captcha Methods *Cipec*.URL: <http://server251.theory.cs.cmu.edu/cgi-bin/sq-pix>, Son Erişim Tarihi: 10.06.2019.

İnternet: Motion Captcha *Cipec*.URL: <http://www.josscrowcroft.com/demos/motioncaptcha/>, Son Erişim Tarihi: 10.08.2019.

İnternet: NuCaptcha *Cipec*.URL: <http://www.nucaptcha.com/>, Son Erişim Tarihi: 10.05.2019.

İnternet: MS Captcha hacked *Cipec*.URL: <http://securitylabs.websense.com/content/Blogs/3063.aspx>, Son Erişim Tarihi: 10.06.2019.

İnternet: MS Captcha hacked *Cipec*.URL: <http://securitylabs.websense.com/content/Blogs/3063.aspx>, Son Erişim Tarihi: 10.06.2019.

İnternet: PWNthca *Cipec*.URL: <http://caca.zoy.org/wiki/PWNtcha>, Son Erişim Tarihi: 15.05.2019.

İnternet: Captcha *Cipec*.URL: <http://captcha.net/>, Son Erişim Tarihi: 20.05.2019.

- İnternet: Google ReCaptcha *Cipec*.URL: <http://www.google.com/recaptcha/learnmore>
<https://www.google.com/recaptcha/intro/invisible.html>
 , Son Erişim Tarihi: 10.08.2019.
- İnternet: Django Simple Captcha is an extremely simple *Cipec*.URL:
<https://github.com/mbi/django-simple-captcha> , Son Erişim Tarihi: 10.08.2019.
- İnternet: Güncel Captcha Çeşitleri *Cipec*.URL: <http://ashamelpro.blogspot.com.tr/>
 , Son Erişim Tarihi: 10.08.2019.
- İnternet: A complicated calculus-based anti-spam CAPTCHA *Cipec*.URL:
<https://nakedsecurity.sophos.com/2011/03/09/a-complicated-calculus-based-anti-spam-captcha/>, Son Erişim Tarihi: 10.08.2019.
- İnternet: reCaptcha good, catCaptcha bad *Cipec*.URL: <http://dailycandor.com/2008/06/>
 , Son Erişim Tarihi: 10.08.2019.
- İnternet: Quantum Random Bit Generator Service: Sign up *Cipec*.URL:
<http://random.irb.hr/signup.php>, Son Erişim Tarihi: 10.08.2019.
- İnternet: Confident CAPTCHA- Image-based CAPTCHA by Confident Technologies
Cipec.URL: https://www.drupal.org/project/confident_captcha, Son Erişim Tarihi: 10.08.2019.
- İnternet: reCAPTCHA: Human-Based Character Recognition via Web Security
 Measures Luis von Ahn,* Benjamin Maurer, Colin McMillen, David Abraham,
 Manuel Blum *Cipec*.URL: <http://www.sciencemag.org/>, Son Erişim Tarihi: 10.08.2019.
- Abdala, K. H. (2017), *Türk üniversitelerinin öğrenci bilgilerini korumak için kullandıkları captcha sisteminin bir analizi*, Yayımlanmış Yüksek Lisans Tezi, Fırsat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ.
- Elatresh, K. (2019), *Üniversite öğrencilerinin CAPTCHA'ya yönelik tutumları* Yayımlanmış Yüksek Lisans Tezi, Atılım Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
- İnternet: Warren S., Ballard B., (2018). Fuzzy Logic *Cipec*.URL:
<https://www.cse.unr.edu/~bebis/CS365/StudentPresentations/FuzzyLogic.ppt>
 , Son Erişim Tarihi: 19.10.2019.
- Tayara, M. (2017). *Animasyonlu metin captchaların sağlamlığı*, Yayımlanmamış Doktora Tezi, Newcastle Üniversitesi Bilgisayar Bilimleri, İngiltere.
- Powell, B.M. (2018). *Enhancing online security with image - based Captchas*, Yayımlanmamış Doktora Tezi, West Virginia Üniversitesi Bilgisayar Bilimleri ve Elektronik Mühendisliği Bölümü, ABD.
- Alharbi, K. (2016). *Friendly security code - based image and audio*, Yayımlanmamış Yüksek Lisans Tezi, King Abdulaziz Üniversitesi Bilgisayar Bilimleri, Suudi Arabistan.

- Greene, M. (2018)., *Large scale Captcha survey* , Yayınlanmamış Yüksek Lisans Tezi, Delaware Üniversitesi Bilgisayar Bilimleri ve Elektronik Mühendisliği Bölümü, ABD.
- Hart, C. (2019)., *Application based bypasses in Google implementation*, Yayınlanmamış Yüksek Lisans Tezi, Utica Enstitüsü, New York.
- Saikirthig A. ve Vaithyasubramanian G., (2016)., *Review on development of some strong visual captchas and breaking of weak audio captcha*, International Conference On Information Communication And Embedded System(ICICES 2016)
- Ramya, G. (2015)., *Captcha as graphical passwords-a new security primitive based on hard AI problems*, Yayınlanmamış Yüksek Lisans Tezi, Troy Üniversitesi Bilgisayar Bilimleri, Troy Alabama.
- Kaur R. (2016)., *A non ocr approach for math captcha design based on boolean algebra using digital gates to enhance web security*, This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference.
- Zhang L., Xie Y., Luan X. Ve He J. (2017)., *Captcha automatic segmentation and recognition based on improved vertical projection*, 2017 9th IEEE International Conference on Communication Software and Networks
- Gutierrez G. (2017)., *A study of online security practices*, Yayınlanmamış Yüksek Lisans Tezi, Arizona Devlet Üniversitesi Bilgisayar Bilimleri, Arizooana.
- Ching M. (2016)., *Task recommendation in crowdsourcing systems* , Yayınlanmamış Doktora Tezi, Hong Kong Çin Üniversitesi Bilgisayar Mühendisliği Bölümü, Çin.
- Yampiro K. D. (2016)., *Establishing human identity through randomly generated lyrics': a comprehensive performer's analysis of robert paterson's captcha and its performance* , Yayınlanmamış Doktora Tezi, James Madison Üniversitesi Müzik Sanatları Bölümü, ABD.
- Robertson W. A. (2018)., *Applications of artificuil intelligence in cyberattacks*, Yayınlanmamış Yüksek Lisans Tezi, Utica Enstitüsü Siber Güvenlik Bölümü, ABD.
- Khalifa W. ve Hasan A. (2016)., *A survey of current research on captcha*, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.7, No.3, June 2016
- Wan S. (2016)., *Protecting Web Contents against Persistent Crawlers*, Yayınlanmamış Yüksek Lisans Tezi, Huazhong Bilim ve Teknoloji Üniversitesi Bilgisayar Bilimleri, Çin

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : ULUHATUN, Necla
 Uyruğu : T.C.
 Doğum tarihi ve yeri : 01.01.1990, Edremit
 Medeni hali : Bekar
 Telefon : 0 (312) 402 22 31
 Faks : 0 (312) 402 22 31
 e-mail : nuluhatun@tsk.tr



Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Adli Bilişim	Devam ediyor
Lisans	Erciyes Üniversitesi / Bilgisayar Mühendisliği	2012
Lise	Van Fen Lisesi	2008

İş Deneyimi

Yıl	Yer	Görev
2014-Halen	Genelkurmay Başkanlığı	Bilgisayar Mühendisi
2013-2014	Emniyet Genel Müdürlüğü	VT Yöneticisi

Yabancı Dil

İngilizce

Yayınlar

Uluhatun, N. ve Çakır, H. (2018). “Güvenlik Kodu Çeşitliliği ile Siber Tehditlere Karşı Güçlü güvenliğin sağlanması” International of Human Sciences Journal ISSN:2458-9489 Volume 15, Issue 3.

Uluhatun, N., Yalçın, Nursel ve Alver, S., (2018). “Diyabetik Retinopati Hastalığının Erken Tespiti İçin Derin Öğrenme ile Retina Görüntülerin Sınıflandırılması” 26th Signal Processing and Communications Applications Conference (SIU) Publisher:IEEE

Hobiler

Yüzme, tiyatro, AI, robotik teknoloji, uzay ve astronomi



GAZİLİ OLMAK AYRICALIKTIR..