International
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 Çakır[1]
Necla Uluhatun[2]

Abstract
Cyberspace also brings about cybercrime, which is evolving along with the rapid progress of technology and internet. Captchars 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 human or bot software.
In this study, a safer Captcha combination test was presented based on Captcha types and Captcha studies. The proposed approach basically consists of three steps. In the first step, the user is asked to test with a simple text-based Captcha to avoid the difficulty of captcha testing. The second stage, when the first stage test is unsuccessful, offers a more complicated captcha test with text and picture. In the third stage, different-based captcha are presented which are more complex than the first two stages and will force the user. This approach makes it easier to distinguish the bot with the user, and the bot program's algorithm can be challenged with the variety of captcha combinations created.
Keywords : Cybecrime; Captcha; Bot, Verification; OCR analysis; Artificial Intelligence; Security; Spam.

(Extended English summary is at the end of this document)

Özet
Siber dünyada, teknoloji ve internetin hızla ilerlemesi beraberinde gelişmekte olan siber suçları da getirmektedir. Güvenlik kodlar (captcha) bu suçları engellemek amacıyla oluşturulan bir güvenlik katmanı olarak kullanılırlar. Bir sisteme giriş yapıldığında girişin kullanıcı tarafından yapılıp yapılmadığının ayırt edilebilmesi için tasarlanmış bir güvenlik mekanizması ve kötü niyetli bot programlarına karşı korunma amaçlı kullanılır. Bu nedenle girişin insan mı yoksa bot yazılımı tarafından mı yapıldığı önem arz etmektedir.
Bu çalışmada, Güvenlik kod (captcha) türleri ve yapılan Güvenlik kod (captcha) çalışmaları baz alınarak daha güvenli bir Güvenlik kod (captcha) kombinasyon testi sunulmuştur. Önerilen yaklaşım temelde üç aşamadan oluşmaktadır. İlk aşamada kullanıcının Güvenlik kod (captcha) ile imtihanını zorlaştırmamak için metin tabanlı basit Güvenlik kod (captcha) ile test edilmesi istenmektedir. İkinci aşamada, ilk aşama testi başarısız olduğunda metin ve resim tabanlı daha zorlaştırılmış Güvenlik kod (captcha) testi sunulmaktadır. Üçüncü aşamada ise ilk iki aşamadan daha karmaşık ve kullanıcıyı zorlayacak farklı tabanlı Güvenlik kodu (captcha) sunulmaktadır. Bu yaklaşım ile kullanıcı ile bot ayırımı daha kolay yapılabilmekte ve oluşturulan Güvenlik kodu (captcha) birleşim çeşitliliği ile bot programlarının algoritmasına meydan okunabilmektedir.
Anahtar Kelimeler : Siber Suç; Güvenlik kodu; Bot; Doğrulama; OCR analizi; Yapay Zeka; Güvenlik; Spam.

[1] Dr. Öğretim Üyesi, Gazi Üniversitesi Gazi Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, hcakir@gazi.edu.tr
[2] Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim Anabilim Dalı, nuluhatun@tsk.tr
Submitted: 2018-03-05 Published: 2018-07-29

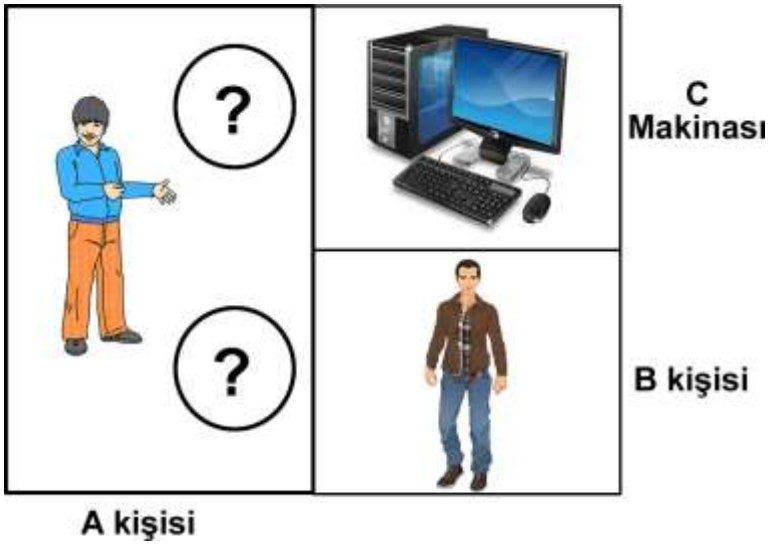
Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201

1. GİRİŞ

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 önüne geçebilmek için doğrulama sistemlerine ihtiyaç duyulmuştur.

Turing Test

İlk olarak 1950 yılında Alan Turing Computing Machinery and Intelligence isimli makalesinde değinmiştir. 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). Şekil 1'de Turing test mantığı gösterilmiştir (McDermott, 2014).



Şekil 1 Turing Test, A Sorgulayan, B ve C Cevaplayan

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 (Von Ahn, Blum, Hopper ve Langford, 2003; Von Ahn, Blum, Hopper ve Langford, 2004). İnsanlar için kolay ama bilgisayarlar için çözümlenmesi zor olan otomatik bir test üretir ve değerlendirir. Bir Güvenlik kodunun (captcha) insan tarafından çözülmesi oranı %90 veya üssü iken bilgisayar programları için yalnızca %1'den daha düşük bir orana ulaşırsa Güvenlik kodu (captcha) güvenli olarak kabul edilmektedir (Bursztein, Martin ve Mitchell, 2011).

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

Bir doğrulama olmaksızın saldırgan kişilerin hedef seçtikleri web sitelerine zarar vermelerini, şifre kurtarma formlarında kaba kuvvet saldırısı kullanarak şifre kırmak, botların mesaj formlarında reklam ya da zararlı paylaşımları çok kolay olabilmektedir. Bu durumların önüne geçilebilmesi için okunması zor, eğri, yamuk, farklı renklerde ya da farklı yöntemlerle değiştirilmiş halde, resim işleme araçları ile botların tanımlayamayacağı ve sadece insanların ayırt edebileceği ve geçebileceği düşünülen bu doğrulama uygulamaları kullanılmaya başlanmıştır.

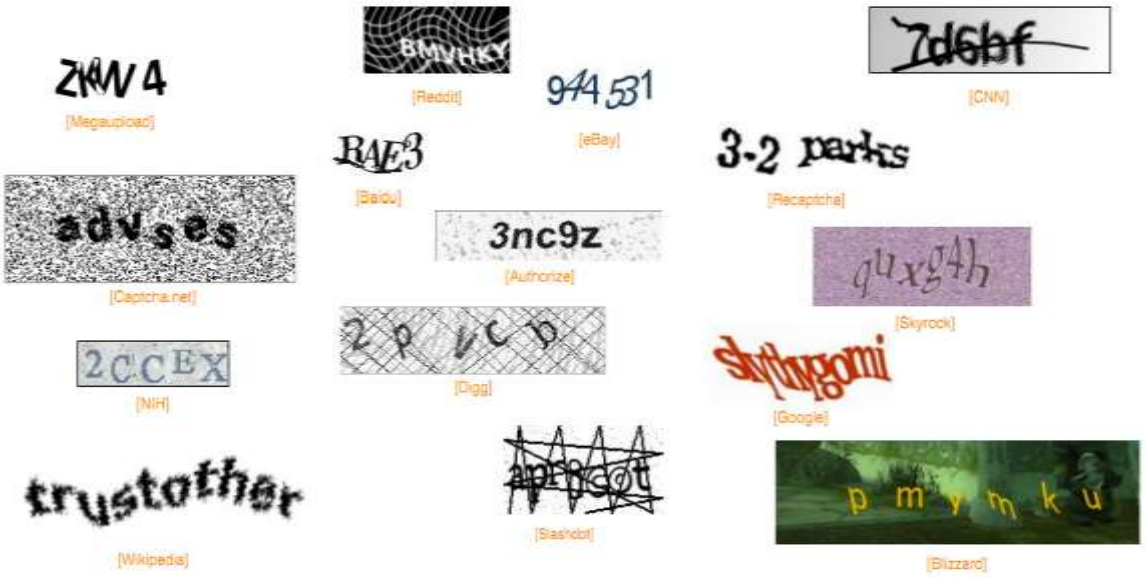
Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201

Güvenlik kodu (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,2015);Demirel, Kılıç,2011). Mevcut Güvenlik kodları (captcha) metin tabanlı, görüntü tabanlı ve ses tabanlı olarak üç kategoriye ayrılabilir. Metin tabanlı Güvenlik kodu (captcha) genellikle İngilizce harfler ve Arapça rakamlara dayanır ve bir makinenin tanınmasını önlemek için karmaşık çarpıklık(sophisticated distortion), rotasyon(rotation) veya gürültü paraziti(noise interference) kullanır.

Karmaşık Çarpıklık: Metin tabanlı captchalarda tanımlanması istenen karakterlerin kompleks bir yapıda içe geçmiş olması durumudur.

Rotasyon: Metin tabanlı captchalardaki karakterlerin açıkça döndürülmüş ve her karakterin dönüş açısı farklı olması durumudur.

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 Karmaşıklığı, rotasyonu ve gürültüsü artırılmış güvenlik kodları (Hugomdq, 2018)

Görüntü tabanlı ve ses tabanlı Güvenlik kodu(captcha) kategorisine kıyasla, metin tabanlı Güvenlik kodu (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 Güvenlik kodu (captcha), Güvenlik kodlarının (captcha) en eski formudur ve insanlar diğer formlara kıyasla metin tabanlı Güvenlik kodu (captcha) tercih etmeye daha eğilimlidirler.

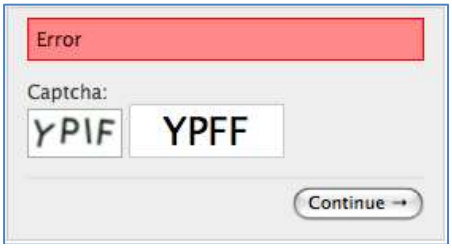
2. GÜVENLİK KODU (CAPTCHA) GELİŞİMİ VE ÇEŞİTLERİ

Güvenlik kodu (captcha) uygulamalarının yayılmasıyla birlikte tersine Güvenlik kodu (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 Güvenlik kodu (captcha)uygulamaları daha karmaşık seviyelere ulaşmaktadır.

Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201

2.1. Basit Güvenlik Kodu (captcha)

Şekil 3'de kullanılan Güvenlik kodu (captcha) çok basit ve gürültüsüz metin tabanlı ilk Güvenlik kodu (captcha) örneklerinden biridir. Bu tür Güvenlik kodları (captcha) kötücül amaçlı uygulamalar tarafından çok özel şekilde hedef alındığında çok kolay aşılabilir.



Şekil 3 Basit Güvenlik kodu (captcha) (Github, 2013)

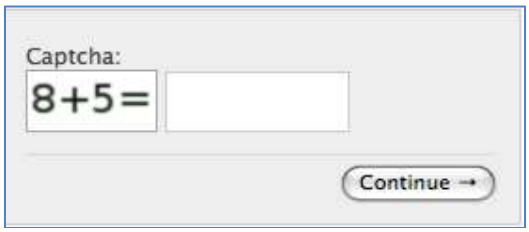
2.2. Güncel Güvenlik kodu (captcha)

Basit Güvenlik kodu (captcha) aşılmaya başlanmasıyla, Güvenlik kodu (captcha) geliştiriciler Güvenlik kodu (captcha) yapılarını daha bulanık, gürültülü, eğri ve görüntüyü farklı simgeler, karalamalar ve şekillerle dolduran daha karmaşık çeşitler geliştirmeye başladılar.

Şekil 4 Güncel Güvenlik kodu (captcha) (Ashamel, 2016)

2.3. Matematik Güvenlik Kodu (captcha)

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

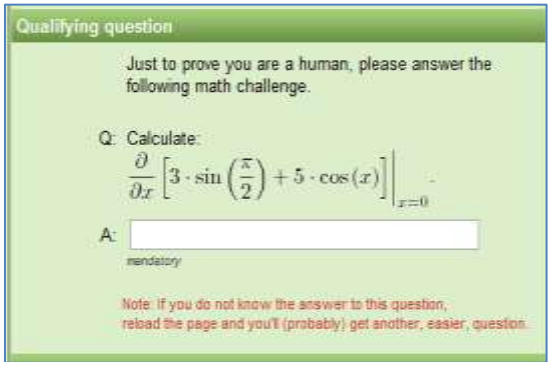


Şekil 5 Matematik Güvenlik kodu (captcha) (Cluley, 2011)

2.4. Karmaşık Güvenlik Kodu (captcha)

Şekil 4'deki Güvenlik kodu (captcha) tasarımları her ne kadar güncel ve güvenli olsa bile, farklı ve daha zorlu tasarımlara ihtiyaç olduğunu savunan, 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 6'daki karmaşık Güvenlik kodu (captcha) geçebilmek için karmaşık modeli çözmesi gerekmektedir.

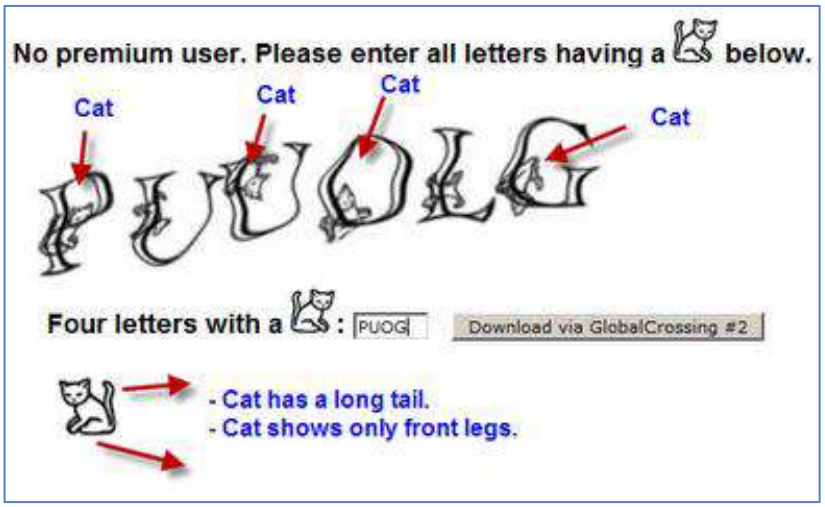
Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201



Şekil 6 Karmaşık Güvenlik kodu (captcha)

2.5. Nesneli Güvenlik Kodu (captcha)

Siber saldırılardan korunmak için sistemlerini korumaya alan tarafların bazıları zor güvenlik kodu(captcha) kullanımını tercih ederken bazıları ise daha basit fakat yine de güvenlikten ödün vermeyeceği düşünülen daha farklı yöntemler kullanmaktadır. Şekil 7'de görülen uyarlama tarzında olduğu gibi klasik farklı açılarla eğriltilmiş harf ve rakam karakterlerinden başka işin içine resimlerin de katıldığı uygulamalar da mevcuttur.



Şekil 7 Nesneli Güvenlik kodu (captcha) (Punk, 2008)

2.6. Resim Güvenlik Kodu (captcha)

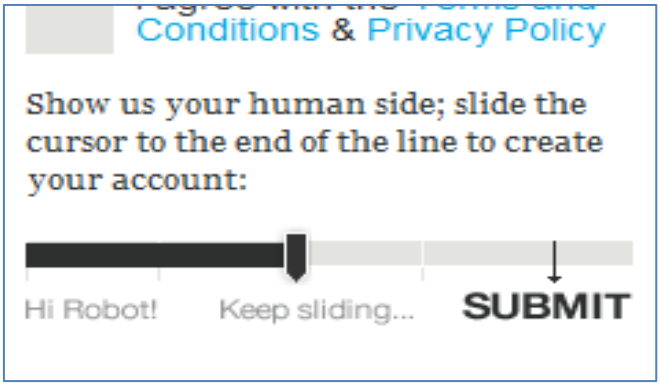
Güvenlik kodu (captcha) geçişi için kullanılan yapılarda anlamsız harf/rakam kombinasyonları kullanma sınırları kaldırıldıktan sonra nesneler Güvenlik kodu (captcha) uygulamalarında daha fazla kullanılmaya başlandı. İnternet hızlarının ve sunucu depolama kapasitelerinin artması ile çok daha güvenli ve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

Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201

Şekil 8 Resim Güvenlik kodu (captcha) (Drupal Security Team, 2010)

2.7. Slider Güvenlik Kodu (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 geçilmesi zor olacaktır. Bu tarz kullanımlar javascript ya da flash teknolojilerini kullandığı için yedek bir doğrulama mekanizmasının olmasını gerektirmektedir.



Şekil 9 Slider Güvenlik kodu (captcha)

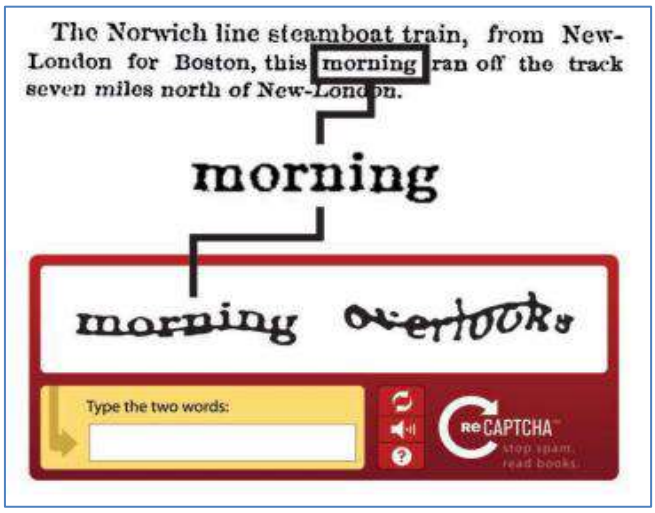
Şekil 8'deki Güvenlik kodu (captcha) uyarlamaları ekranla etkileşime geçilmesi gereken uyarlamalar güvenlikli olmasına rağmen uygulama zorlukları sebebiyle pek tercih edilmemektedir.

2.8. reCaptcha

Google Güvenlik kodu (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. Metin tabanlı bilgilerin sayısal halde edilmesinde kullanılmak üzere elde edilen OCR çıktılarını kullanıcılara yönlendirilecek şekilde reCaptcha olarak yeniden düzenledi. Doğrulama aşamasında daha önceden başkaları tarafından doğrulanmış bir kelime ve ikinci bir tanımlanamamış kelime gösterilmektedir; önceden tanımlanmış kelimeyi eşleştirerek insan ayrımı yapıldıktan sonra ikinci kelimeyi de Google Kütüphaneleri ve başka reCaptcha doğrulamaları için tanımlamış olmaktadır. (Bkz. Şekil 10) Bu sayede Güvenlik kodu (captcha) uygulamalarının doğrulanması sırasında hem daha güvenilir sistem geçişi sağlanmıştır.

Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201

Ayrıca captcha metni okuma sırasında kaybedilen zaman, kullanıcılara kitap okutturmak gibi bir fayda sağlamaktadır (Luis, Maurer, McMillen, Abraham ve Blum, 2008).



Şekil 10 reCaptcha

3. GÜVENLİK KODU (CAPTCHA) GENEL MANTIĞI VE İŞLEYİŞİ

Güvenlik kodu (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.

Güvenlik Kodu (captcha) Resim Yaratma Adımları:

- Bitmap nesnesi yaratılır
- Bu bitmap nesnesinin yazı tipi, yazı biçimi gibi özelikleri 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 Güvenlik kodu (captcha) gelişimi başlamıştır(Yan ve El Ahmad, 2007; Yan ve El Ahmad, 2008).

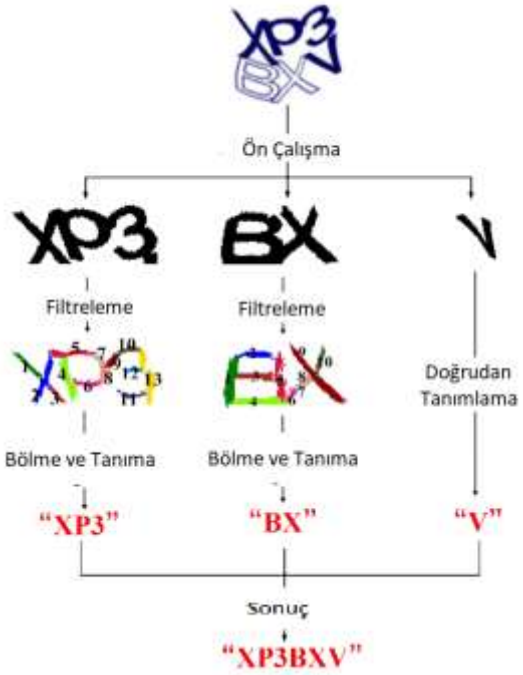
Karşıt uygulamalar ile yarışı sırasında Güvenlik kodu (captcha) her ne kadar değişik uygulama tarzları ortaya çıkmış olsa da temelde uygulamaların mantığı hep aynıdır. Bu mantık Turing testine dayanmaktadır.

Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201

4. GÜVENLİK KODU (CAPTCHA) KODUNUN KIRILMASI

Güvenlik kodu (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 Güvenlik kodu (captcha) türü özelliklerine göre fazlara ayrılmalı ve reCaptcha botu faz değiştirerek sonuca gitmelidir. En belirgin özellikleri ilk adımlarda eleyerek ilerlemek en mantıklısı olacaktır.

Örneğin klasik Güvenlik kodu (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 4' te 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(Pretend We'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 (PWNthca, 2017).



Şekil 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.

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

Güvenlik Kodu (captcha) Kırma Temel Algoritması

Karakter Tanıma ve Görüntü işleme

Güvenlik kodu (captcha) bitmap olarak aldıktan sonra bu bitmap dosyasını sayısal bir resme dönüştürür.

Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201

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. Güvenlik kodu (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 büyütmektir. Sayısal bir resimin aşındırılmasıdır.

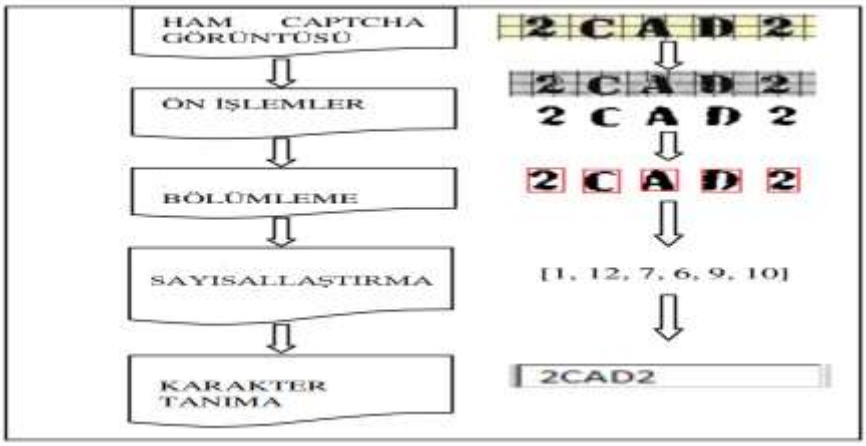
Filtreler

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

Karakterin Tanınması

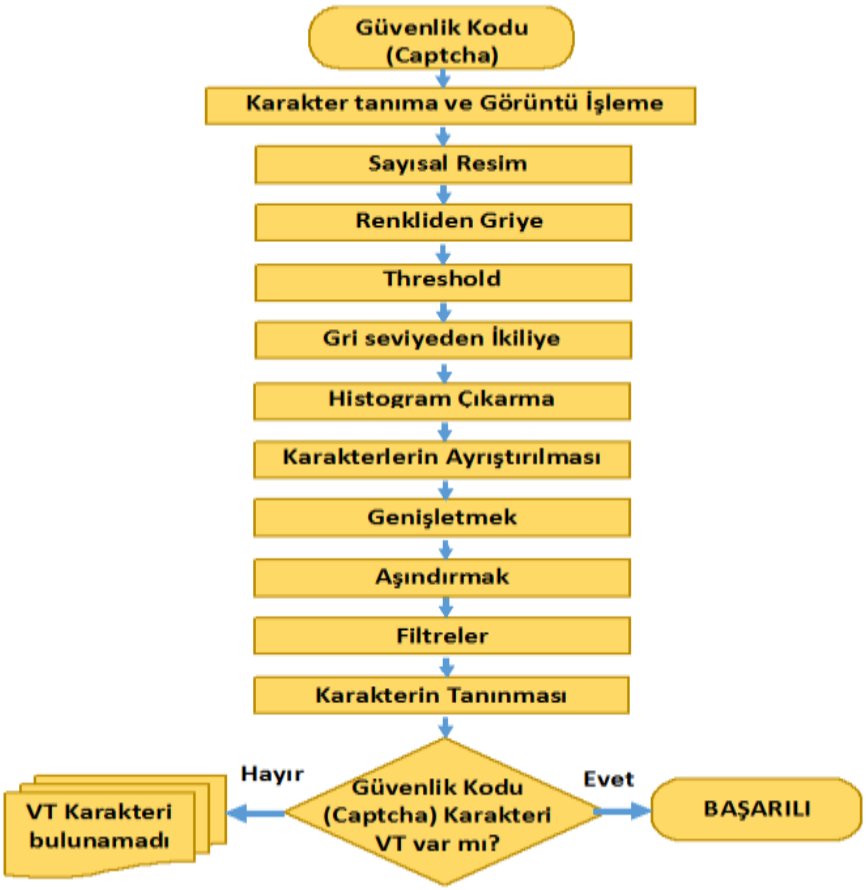
Karakter farklı görüntü işleme tekniklerinden geçtikten sonra histogramla ayrılarak belirlenmiş olan threshold değerine göre ikili (binary) diziye çevrilmesidir.

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



Şekil 12 Captcha Kırma Temel Adımları(Eken, Sayar, 2015)

Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201



Şekil 13 Güvenlik kodu (captcha) Kırma Şeması

5. GÜVENLİK KODU (CAPTCHA) YAKIN GELECEĞİ

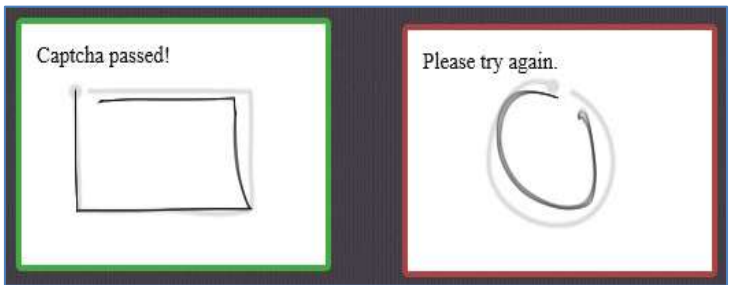
Güvenlik kodu (captcha) uygulamaları artık spamı engellemek isterken işlevselliğini kaybedip kullanıcıyı engelleyen ve canını sıkan yapısından sıyrılıp ReCaptcha örneğindeki gibi daha modernize ve işlevsel duruma gelirken, bir amaç uğruna çalışır hale gelmiştir. Bu her ne kadar isteğe bağlı bir geliştirme 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 Güvenlik kodu (captcha) sistemi %35'lik başarı oranıyla aşılmış (Kdawson, 2008) ve bu oran düşük gibi gözükse dahi çeşitli yollarla 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 çıtasını bir kademe daha yükseltmektedir ve bu, sonuçta yazılım dünyasının, insanlığın kazancınadır. Resim Güvenlik kodu (captcha) ve sesli dinleyerek doğrulama olanağı geliştirmeleri bunun kanıtıdır; klasik uyarlamanın dışında olan ve işlevselliği arttırmaya çalışan bu iki yaklaşım da aşılarak daha sonrasında çıtayı yeniden yükseltmiştir (Mims, 2011; Kleiner, 2008).

Bugünlerde yaygın olarak kullanılmasa da ileride video Güvenlik kodu (captcha) uygulamalarının benimseneceği ve gelişen dokunmatik ekran sistemleri ile resim Güvenlik kodu (captcha) gelişip el işareti, çizim doğrulamalarının ve uyarlamalarının (Bkz. Şekil 14, 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 Güvenlik kodu (captcha) servisinin kırılmış olması bunun en büyük göstergesidir (Sharf,2012).

Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201



Şekil 14 Çizim Güvenlik kodu (captcha)

Şekil 15 Hareket Güvenlik kodu (captcha)

3D Güvenlik kodu (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 Güvenlik kodunu (captcha) başarıyla çözmektir.

Şekil 16 3D Güvenlik kodu (captcha)

Şekil 17 Key Güvenlik kodu (captcha)

Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201

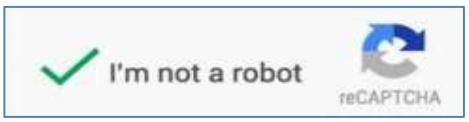
Hoş ve keyifli bir Güvenlik kodu (captcha) oyunu ile ziyaretçileri eğlendirir. Resimdeki eksik parçaları tamamlanmasını sağlayan ufak bir bulmaca oyunudur.

Şekil 18 PlayThru Güvenlik kodu (captcha)

PlayThru - HTML5 oyun tabanlı bir CPATCHA, İnsan olduğunuzu ispatlamak için oyunu başarılı bir şekilde tamamlamanız gerekir. İngilizce'yi anlayan her insanın kolayca bitirmesi çok zor olmayan bir Güvenlik kodudur.

Google Yeni Güvenlik Kodu (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).



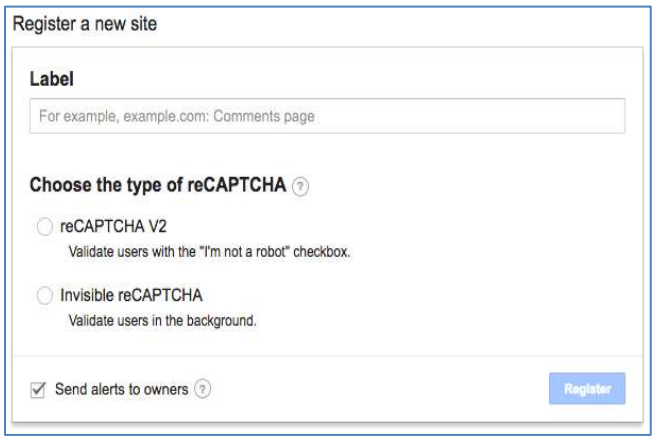
Şekil 19 reCaptcha

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, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201



Şekil 20 Invisible reCAPTCHA

6. SİBER TEHDİTLERE KARŞI GÜVENLİK KODU (CAPTCHA) TEST ÇALIŞMASI

Güvenlik kodu (captcha) genel olarak sistemlere giriş yapmaya çalışan kötücül bot yazılımlarına karşı fiziksel dünyadaki gibi güvenliği sağlayan, izinsiz girişi engelleyen bir zırh gibidir. Bu bağlamda değerlendirildiğinde fiziksel korumayı sağlayan zırhlar bireyin taşıyabileceği hafiflikte olur ve istenilen tasarım ve darbelere karşı korunaklı olursa o kadar çok tercih edilir. Güvenlik kodu (captcha)'da tıpkı zırhlar gibi dayanıklı, sistemin taşıyabileceği kadar az enerji harcar ve kullanıcı dostu olursa talep edilmesi o kadar yüksek olacaktır.

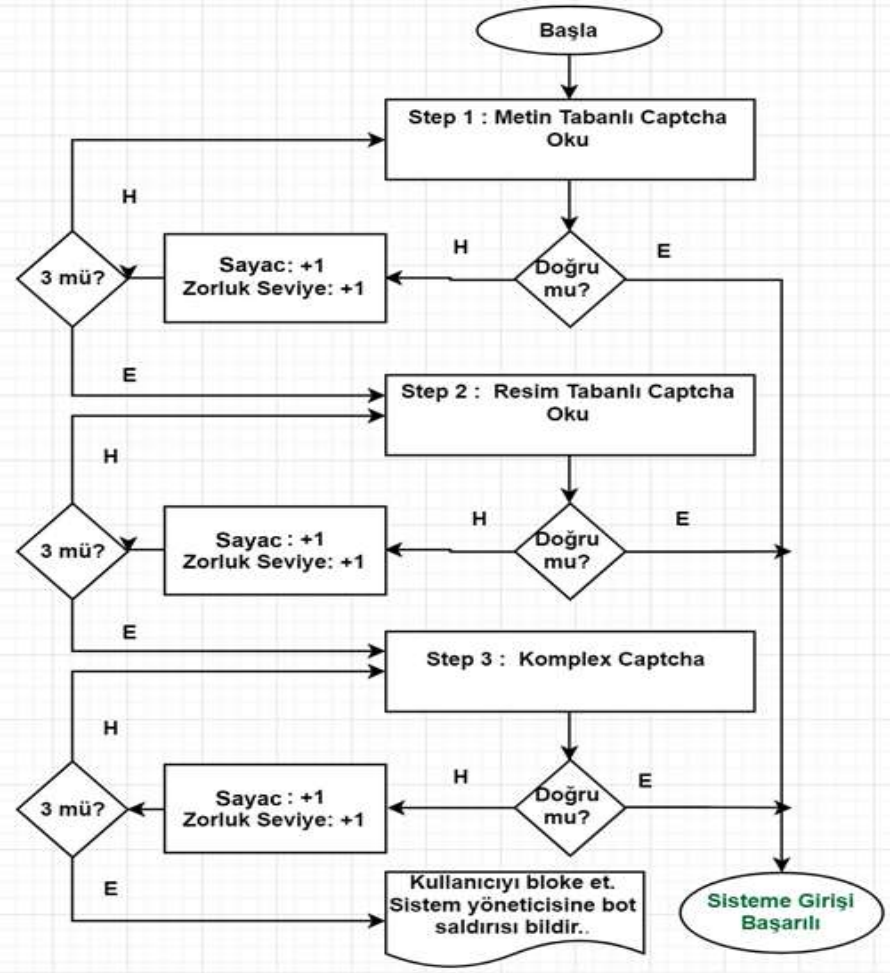
Güvenlik kodu (captcha) geçmişten günümüze kadarki gelişimine bakıldığında temel mantığı 3 temel kategoriye dayanmaktadır. Bunlar metin, ses ve görüntüdür. Bunlar veya bunların birleşimleri alınarak çeşitli Güvenlik kodu (captcha) oluşturulmuştur. Bu oluşturulan Güvenlik kodu (captcha) çoğu gelişen teknolojik gelişmelerle birlikte özelikle OCR sistemleri ve makine öğrenme, sinir ağları, derin öğrenme yöntemleriyle en zor ve karmaşık Güvenlik kodu (captcha) bile bot yazılımları tarafından kırılabilmiştir. Bunların kullanılmaya başlanması ile Güvenlik kodu (captcha) kırılması ve gelişen teknolojiye paralel olarak gelişen ve hedeflenen Güvenlik kodu (captcha) modeline doğru bir Güvenlik kodu (captcha) evrimi gerçekleştiği göktedir. Gelişen teknoloji sistem güvenliğini daha etkin kılmak için uğraşılırken karşı taraf denilen kötücül amaçlılar bu gelişen teknolojiyi kullanarak daha etkin bot yazılımları yapmaktadırlar.

Aşılan ve kırılan bir uyarlama sonrası daha karışık ve güvenlikli bir uygulamanın geliştirilmesi kaçınılmaz iken Güvenlik kodu (captcha) bu denli gelişmesi evrimleşen DeCaptchların oluşmasına sebep olmaktadır. Daha gürültülü, parazitli ve zor ses Güvenlik kodunun (captcha) aşılabilmesi ve daha gürültülü ortamlarda dahi kullanıcı sesini tanımlayabilecek yazılımlar demektir.

Hızla gelişen siber dünyada evrimleşen karışık Güvenlik kodu (captcha) oluşturulurken buna bağlı olarak gelişen bot yazılımları da daha zeki olmaya başlamışlardır. Geliştirilen karmaşık Güvenlik kodu (captcha) ve kullanıcı dostu ara yüzler (javascript, html, flash gibi ihtiyaçların doğması..) tasarlanmaktır. Güvenlik kodu (captcha) testlerin zorlaşması ve kullanıcının testi geçmesinde zorlanmasına bağlı oluşan isteksizliğin artması gibi problemler göz önünde bulundurularak bu çalışma hazırlanmıştır.

Çalışmada mevcut Güvenlik kodu (captcha) katmanları kullanılarak kullanıcıya 3 adımda seviye seviye zorluğu artan bir Güvenlik kodu (captcha) birleşimi geliştirilmiştir. Çalışmanın algoritması Şekil 21'deki gibidir.

Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201



Şekil 21 Akış Diyagramı

Bunun sonucunda kullanıcının sistemde kalma süresini uzatmadan ve kullanıcıya sanal hırsız muamelesi göstermen temel Güvenlik kodu (captcha) seviyesinden başlayarak kullanıcının insan mı bot mu olduğu Güvenlik kodu (captcha) çeşitliliğinden yararlanılmaktadır. Dönen sonuca göre gittikçe zorlaştırılan Güvenlik kodu (captcha) bir üst aşamaya geçerek zorlaştırılan test ile sistem güvenliği sağlanmaktır. Böylece sistem ve kullanıcı dostu bir Güvenlik kodu (captcha) testi oluşturulmuş olunur. Bu çalışmadaki ana amaç bot saldırılarında Güvenlik kodu (captcha) çeşitliliğini artırarak bot yazılımlarının algoritma yapısını zorlayarak meydan okumak ve böylece daha güvenli bir Güvenlik kodu (captcha) testini sağlamaktır.

7. SONUÇ

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 Güvenlik kodu (captcha) sistemleridir.

Güvenlik kodu (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 zeka ile çözülebilmesi olayı Güvenlik kodu (captcha) doğrulama sahnesinden daha farklı bir boyuta taşımaktadır(Kleiner, 2008). Güvenlik kodunu (captcha) bu tarz yapay sinir ağları ile geliştirme yapan kişiler için de günden güne gelişen ve zorlaşan iyi bir test aracı olduğu ortadadır. Gelişimi

Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201

sırasında farklı özellikler kazansa dahi bu özellikler daha önceki örneklerde ki gibi yine yeni alanlarda gelişmelere yön verecektir ve amacından fazlasına hizmet etmeye devam edecektir.

Önerilen yaklaşımla Güvenlik kodu (captcha) taban türleri baz alınarak zorluk seviyesine göre adımlar halinde kullanıcıyı bunaltmadan, sistemi zorlamadan işlemler yaptırılmaktadır. En önemli dönüt ise oluşabilecek bot saldırılarında kullanılan Güvenlik kodu (captcha) çeşitliliği ile kötücül yazılımın algoritmik yapısını zorlayarak sistemi korumaktadır. (Gao, Tang ve Liu, 2017)'de 2017 yılında Microsoft Güvenlik kodu (captcha) yapılan saldırıda kullanılan algoritma tek tür Güvenlik kodu (captcha) yapısını aşabilecek şekilde tasarlandığı ve kırıldığı göz önünde bulundurulduğunda Güvenlik kodu (captcha) çeşitliliği ile bot yazılımın algoritmasını zorlamanın sistem güvenliği açısından önemi daha iyi anlaşılacaktır.

KAYNAKÇA

Ahn1,& L. Blum1,M.& Hopper1, N. J. & Langford2, J. (2003)*CAPTCHA:Using Hard AI Problems For Security* Computer Science Dept., Carnegie Mellon University, Pittsburgh PA 15213, USA IBM T.J. Watson Research Center, Yorktown Heights NY 10598, USA

Ashamel, S. (2016) "Güncel Captcha Çeşitleri" Web Sitesi http://ashamelpro.blogspot.com.tr/ Erişim tarihi: 15.05.2016

Bursztein, E.& Martin, M. & Mitchell, J.(2011) *Text-based captcha strengths and weaknesses,* in Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011, (pp. 125–138)

Captcha, (2017) "Captcha" Web Sitesi http://captcha.net/ Erişim tarihi: 15.05.2018

Chellapilla, K.& Larson, K. & Simard, P. Y. & Czerwinski, M.(2005) *Building segmentation based human-friendly human interaction proofs (hips),* in Human Interactive Proofs. Springer, 2005, (pp. 1–26.)

Cluley, G. (2011) "A complicated calculus-based anti-spam CAPTCHA" Web Sitesi https://nakedsecurity.sophos.com/2011/03/09/a-complicated-calculus-based-anti-spam-captcha/ Erişim tarihi: 15.05.2018

Demirel C.& Kılıç, D. (2011) "New Captcha Methods" Conference: XVI. Türkiye'de Internet Konferansı, At İzmir Web Sitesi Erişim tarihi: 1511.2017 https://www.researchgate.net/publication/265258826_Captcha_ile_Guvenlige_Genel_Bakis

Drupal Security Team, (2010) "Confident CAPTCHA - Image-based CAPTCHA by Confident Technologies" Web Sitesi https://www.drupal.org/project/confident_captcha Erişim tarihi: 15.05.2017

Eken, S.& Sayar, A.(2015) *Capcha Karakterlerinin Yapay Sinir Ağları Kullanılarak Tanınması,* IEEE Conference Paper Template

Gao, H.& Tang, M. & Liu, Y. (2017)Research on the Security of Microsoft's Two-layer Captcha IEEE Transactions on Information Forensics and Security (Volume: 12, Issue: 7, July 2017)

Github,(2013) "Django Simple Captcha is an extremely simple" Web Sitesi https://github.com/mbi/django-simple-captcha Erişim tarihi: 15.05.2017

Google, (2017) "ReCaptcha" Web Sitesi https://www.google.com/recaptcha/intro/invisible.html Erişim tarihi: 15.05.2017

Hall, L. (2015)"Motion Captcha" Web Sitesi https://gdblogs.shu.ac.uk/b2017077/2015/03/09/600-people-a-captcha-approach-to-typography/ Erişim tarihi: 15.11.2017

Hugomdq, (2018) "Captcha vs ReCaptcha" Web Sitesi http://hugomdq.com/captcha-vs-recaptcha/ Erişim tarihi: 01.05.2018

IRB, (2018) "Quantum Random Bit Generator Service: Sign up" Web Sitesi http://random.irb.hr/signup.php Erişim tarihi: 15.05.2018

James, H.M. (2001) *The Status and Future of the Turing Test,* Minds and Machines, 11: 77–93.

Kdawson on Tuesday January 29, 2008 "Yahoo Captcha Hacked" Web Sitesi. http://it.slashdot.org/story/08/01/30/0037254/yahoo-captcha-hacked Erişim tarihi: 05.02.2018

Kleiner, K. (2008) "Image Security Captchas Hacked" Web Sitesi. http://www.technologyreview.com/web/21519/page1/ Erişim tarihi: 25.01.2018

Kumar, C. & Kevin, L. & Patrice, S. Y. & Mary, C. (2005) *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.

Luis, V. A.& Maurer, B. & McMillen, C. & Abraham, D. & Blum , M. (2008) *reCAPTCHA: Human-Based Character Recognition via Web Security* http://www.sciencemag.org/

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

Mims, C. (2011) "Audio Security System Cracked" Web Sitesi. http:// www. technologyreview.com/computing/37690/?mod=related Erişim tarihi: 05.02.2018

NuData (2017) "NuCaptcha" Web Sitesi http://www.nucaptcha.com/ Erişim tarihi: 15.11.2017

Punk, D. (2008) "reCaptcha good, catCaptcha bad" Web Sitesi http://dailycandor.com/2008/06/ Erişim tarihi: 15.05.2017

PWNthca,(2017) "Captcha Decoder" Web Sitesi http://caca.zoy.org/wiki/PWNtcha Erişim tarihi: 15.05.2018

Sharf, E. (2012) "MS Captcha hacked" Web Sitesi https://blogs.forcepoint.com/security-labs/trojan-caught-camera-shows-captcha-still-security-issue Erişim tarihi: 15.12.2017

Von Ahn, L. & Blum, M. & Hopper, N. J. & Langford, J. (2003) *Captcha: Using hard ai problems for security*, in Advances in CryptologyIEUROCRYPT *2003*. (pp. 294–311) Springer

Von Ahn, L. & Blum, M. & Hopper, N. J. & Langford, J. (2004) *Telling humans and computers apart automatically,* Communications of the ACM, vol. 47, no. 2, 2004 (pp. 56–60)

Yan, J. & El Ahmad, A. S.(2008) *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)

Yan, J. & El Ahmad, A. S. (2007) *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. & El Ahmad, A. S. (2008) *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.)

Extended English Summery

Captcha (Full Automatic General Turing Test for Human and Computer Separation) is used to prevent automatic recording, spam or malicious bot programs.It produces and evaluates an automated test that is easy for humans but difficult for computers to solve. Captcha is considered safe if a Captchan reaches a rate of 90% or lower for humans and only less than 1% for computer programs.

The existing Captchas can be divided into three categories: text based, image based and audio based. Text-based Captcha is usually based on English letters and Arabic numbers and uses complex skewness, rotation or noise parasites to prevent recognition of a machine. Compared to the last two Captcha categories, text based Captcha is the most widely used scheme. This widespread use is due to its obvious advantages. The problem problem that is intuitive for users around the world is the text; In general, people can recognize English letters and Arabic numbers, so the text based Captcha has few localization issues; also, text based Captcha is the oldest form of Captchas and people tend to prefer text based captcha compared to other forms.

In parallel with the fast-paced development of technology, cyber warfare is increasing proportionally in the virtual world. In this context, the simultaneous development of positive and negative aspects of technology has taken various security importance in order to make users more comfortable and safe circulation in the virtual world. The most basic of these is the captcha systems. Cyberspace also brings about cybercrime, which is evolving along with the rapid progress of technology and internet. Captchars 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 human or bot software.

Çakır, H., & Uluhatun, N. (2018). Güvenlik kodu çeşitliliği ile siber tehditlere karşı güçlü güvenliğin sağlanması. *Journal of Human Sciences*, *15*(3), 1414-1430. doi:10.14687/jhs.v15i3.5201

In this study, a safer Captcha combination test was presented based on Captcha types and Captcha studies. The proposed approach basically consists of three steps. In the first step, the user is asked to test with a simple text-based Captcha to avoid the difficulty of captcha testing. The second stage, when the first stage test is unsuccessful, offers a more complicated captcha test with text and picture. In the third stage, different-based captcha are presented which are more complex than the first two stages and will force the user. This approach makes it easier to distinguish the bot with the user, and the bot program's algorithm can be challenged with the variety of captcha combinations created.

Systems that can be neglected by simple examples of artificial intelligence rather than the simpler methods that can be overcome more difficult than the result of evolving in cases where the security code (captcha) applications are inadequate are emerging, and the problem of solving the artificial intelligence with these difficulties can be solved in a different dimension than the captcha verification scene carry. The security code (Captcha) is also a good test tool for those who develop with such artificial neural networks. Even if they acquire different characteristics during their development, these characteristics will continue to evolve in the new areas as in the previous examples and will continue to serve the purpose more.

Based on the suggested approach, the security code (Captcha) bases on the difficulty level based on the types of the steps, without overwhelming the user, the system is done without force. The most important feedback is to protect the system by forcing the algorithmic structure of the malicious software with the diversity of the security code (captcha) used in the bot attacks. In 2017, when the attack algorithm used in Microsoft security code (Captcha) was designed to overcome a single type of security code (Captcha) and it was broken, it is more important in terms of system security to enforce the algorithm of the bot software with the diversity of security code (Captcha) It will be understood.

As a result, the captcha models used from the past to the present day were investigated. Bot attacks and variations on Captcha models are also taken into consideration. As a result of this work, it has been found that bot aggression is difficult with the increase of existing captcha varieties.
In this context, the captcha codes that are becoming increasingly complex in a way that will force user friendly and bot programs are presented in the study. When there are incorrect captcha entries, the level of complexity is increased and the bot attack programs are forced by the combination of captcha. We see that this is a preferable combination because it is user-friendly and it forces bot programs.