METİN VE GRAFİKSEL ÖĞELERİ BİRLEŞTİREN YENİ BİR PAROLA TABANLI KİMLİK DOĞRULAMA YÖNTEMİ

MURAT AKPULAT

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

TOBB EKONOMİ VE TEKNOLOJİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

TEMMUZ 2012
ANKARA

Fen Bilimleri Enstitü onayı

_____

Prof. Dr. Ünver KAYNAK
Müdür

Bu tezin Yüksek Lisans derecesinin tüm gereksinimlerini sağladığını onaylarım.

_____

Doç. Dr. Erdoğan DOĞDU
Anabilim Dalı Başkanı

Murat AKPULAT tarafından hazırlanan METİN VE GRAFİKSEL ÖĞELERİ BİRLEŞTİREN YENİ BİR PAROLA TABANLI KİMLİK DOĞRULAMA YÖNTEMİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

_____

Doç. Dr. Kemal BIÇAKCI
Tez Danışmanı

Tez Jüri Üyeleri

Başkan :Yrd. Doç. Dr. Muhammed Fatih DEMİRCİ _____

Üye : Doç. Dr. Kemal BIÇAKCI _____

Üye : Doç. Dr. Bülent TAVLI _____

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

MURAT AKPULAT

Üniversitesi : **TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü : **Fen Bilimleri**
Anabilim Dalı : **Bilgisayar Mühendisliği**
Tez Danışmanı : **Doç. Dr. Kemal BIÇAKCI**
Tez Türü ve Tarihi : **Yüksek Lisans – Temmuz 2012**

Murat AKPULAT

METİN VE GRAFİKSEL ÖĞELERİ BİRLEŞTİREN YENİ BİR PAROLA TABANLI KİMLİK DOĞRULAMA YÖNTEMİ

ÖZET

Güvenlik sistemlerini bir bütün olarak ele aldığımızda, bu bütünün ilk ve belki de en önemli parçası kimlik doğrulamadır. Özel donanım gerektirmeme ve kullanım kolaylığı gibi sebeplerden dolayı günümüzde en yaygın kullanılan kimlik doğrulama yöntemi şifre (parola) tabanlı olanlardır. Ancak kullanıcıların tahmin edilmesi kolay şifreler seçmesi ciddi güvenlik problemlerini beraberinde getirmektedir. İnsanın resim hafızasının sözel hafızadan daha üstün olması gerçeğinden yola çıkılarak son yıllarda pek çok grafiksel parola yöntemleri geliştirilmiş fakat bu yöntemler pratik uygulamalarda henüz klasik metin parolaların yerini alamamıştır. Bu çalışmada alışkanlık bağlamında daha az değişiklik gerektiren ve hem metin hem grafiksel öğeler içeren yeni bir parola tabanlı kimlik doğrulama yöntemi önermekteyiz. Yaptığımız deneysel çalışmalar Yaz&Tıkla ismini verdiğimiz yeni yöntemin hem uzun dönem hatırlanabilirlik hem de kullanıcı memnuniyeti açısından sadece metin ve sadece grafik tabanlı parola yöntemlere oranla daha başarılı olduğunu göstermektedir.

Anahtar Kelimeler: Kullanışlı Güvenlik, Grafik Şifre, Parola, Kimlik Doğrulama

University : **TOBB Universty of Economics and Technology**
Institute : **Institute of Natural and Applied Sciences**
Science Programme : **Computer Engineering**
Supervisor : **Associate Professor Dr. Kemal BIÇAKCI**
Degree Awarded and Date : **M.Sc. – July 2012**

Murat AKPULAT

A NEW PASSWORD BASED AUTHENTICATION METHOD COMBINING TEXTUAL AND GRAPHICAL ELEMENTS

ABSTRACT

When security systems are considered as a whole, the first and perhaps the most important part is authentication. Due to reasons such as not requiring special hardware and ease of use, the most used authentication methods are the ones based on passwords. Yet, the fact that users choose easy-to-guess texts as passwords makes all the precautions the security systems try to take void. Based on the fact that human's picture memory is superior to his verbal memory, many graphical password methods were developed but these methods have not replaced text based passwords in practice. In this study, a new password based authentication method, which is based on both text and graphical elements and that needs fewer changes in user behaviour, is put forward. In the empirical studies carried out, the new method so called "Type&Click" is found to be more successful in terms of long-term memorable and user satisfaction when compared to text only and graphical only password methods.

Keywords: Usable Security, Graphical Password, Password, Authentication

TEŞEKKÜR

Yüksek lisans eğitimimin ilk gününden itibaren gösterdiği ilgi ve içtenlikten dolayı kıymetli hocam Doç.Dr. Kemal BIÇAKCI'ya tüm kalbi duygularımla şükranlarımı sunuyorum. Sizden çok şey öğrendim, örnek kişiliğiniz hayatım boyunca rehberim olacaktır.

Beni kırmayıp tez savunmamı değerlendirmeyi kabul eden Doç.Dr.Bülent TAVLI ve Yrd.Doç.Dr. Muhammed Fatih DEMİRCİ hocalarıma, yardımlarını esirgemeyen asistan arkadaşım Uğur ÇİL'e,

Yüksek lisans dönemi boyunca birçok konuda yardımlarını istediğim ve gönülden yardımcı olduklarını gördüğüm Gümüşhane Üniversitesi Kelkit Aydın Doğan Meslek Yüksekokulunun çok kıymetli öğretim elemanları ve idari personeline,

Hayatımın her safhasında güven ve desteklerleriyle yanımda olan canım ailem ve sevgili eşime,

Minnet ve şükranlarımı sunuyorum. Teşekkür ederim.

İÇİNDEKİLER

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

KISALTMALAR

Kısaltmalar	Açıklama
PCCP	Persuasive Cued Click-Points
CCP	Cued Click-Points
NIST	National Strategy for Trusted Identities in Cyberspace

BÖLÜM 1 - GİRİŞ

Hızla gelişen bilişim sistemleri kullanıcıların sosyal ve mesleki hayatlarını oldukça rahatlatmıştır. Her kesimin ihtiyaç duyduğu doğru bilgiyi en hızlı ve en kolay bir şekilde sağlamak, bilişim sistemlerinin amaçlarından bir tanesi olmuştur. Bilgiye kolay ve hızlı erişim, beraberinde birtakım güvenlik ihtiyaçlarını doğurmuştur. Dünyanın en geniş ve kullanıcısı en fazla haberleşme ağı olan internette de kullanıcıların bazı bilgilere ulaşabilmek için birtakım izin ve kurallara tabi olması şart haline gelmiştir. Sadece kendi kullanıcılarına hizmet vermek isteyen bazı internet siteleri, sayfalarına ekledikleri bir takım kimlik doğrulama mekanizmaları sayesinde sadece kayıtlı (izinli) kullanıcılarının erişimine izin vermişlerdir. Kimlik doğrulama mekanizmaları genel olarak şu başlıklar halinde toplanabilir:[1]

- Kullanıcının ne bildiği;

Günümüzde çok yaygın olarak kullanılan, kullanıcı adı ve sadece kullanıcının bildiği bir parola ile kullanıcı sisteme kendini tanıtmış olur.

- Kullanıcının kim olduğu;

Kullanıcı, bu mantıkla hazırlanan bir kimlik doğrulama mekanizmasında, kendisine has olan biyometrik bazı özelliklerini (parmak izi, retina taraması vb.) ile kendini sisteme tanıtır. Kullanıcılar herhangi bir şifreyi ezberleme zorunluluğu yada herhangi bir kartı yanında taşıma zorunluluğu olmaksızın, biyometrik özellikleri sayesinde sisteme kendilerini tanıtabilirler. Ancak bu sistemlerin maddi külfetlerinin yanında, biyometrik bazı verilerin kopyalanabilir olması, mahremiyeti ortadan kaldırması, fiziksel engelli kullanıcılar için kullanışsız olması gibi faktörlerden pek fazla tercih edilmemektedir.

- Kullanıcının ne taşıdığı;

Bu sistemde kullanıcılar yanlarında taşıdıkları akıllı kart yada program kilidi gibi sisteme özel fiziksel bir nesne ile kendilerini sisteme tanıtırlar.

Bu tez de genel amaç "kullanıcının ne bildiği" mantığıyla hazırlanan kimlik doğrulama sistemlerinin incelenmesi ve mevcut sistemlere alternatif olarak geliştirilen Yaz&Tıkla yönteminin deney sonuçlarını sunmaktır [2].

Ayrıca yeni yöntemin kullanılabildiğini daha iyi anlama adına yapmış olduğumuz deneysel çalışmaların sonuçları sunulacaktır.

1.1 Teze Genel Bakış

Bu tez çalışması aşağıda belirtilen konu başlıklarında sunulmuştur.

Bölüm 2'de genel bilgilere yer verilmiştir. Konuyla ilgili temel terimler, daha önce yapılan çalışmalar maddeler halinde sunulmuştur. Bölüm 3'de geliştirilen alternatif yöntem ve karşılaştırılacak PCCP ve metin tabanlı yöntem tanıtılmıştır. Bölüm 4'de alternatif yöntemi diğer yöntemlerle karşılaştırmak için geliştirilen deney metodolojisi tanımlanmış, deney süreci açıklanmıştır. Bölüm 5'de deney sürecinden elde edilen veriler yorumlanmıştır. Bölüm 6'da geliştirilen yöntemin sonuçları özetlenmiştir. Bölüm 7'de bu çalışma sırasında faydalanılan bilimsel eserler sıralanmıştır. Son olarak, Yaz&Tıkla yöntemini son haline ulaştırmadan önce yöntemin gelişim evreleri iki ek ile anlatılmıştır.

1.2 Bu Araştırmanın Temel Amacı

Grafik tabanlı şifre yöntemlerinin yer edinmeye çalıştığı parola tabanlı kimlik doğrulama sistemleri çerçevesinde, geliştirdiğimiz grafiksel ve metinsel öğeleri beraber barındıran alternatif yöntemin deneysel yöntemler kullanılarak bilhassa kullanılabilirlik kriteri baz alınarak incelenmesidir.

BÖLÜM 2 - GENEL BİLGİLER

Güvenlik sistemleri, yetkili kişilerin sisteme girişine izin verecek ve yetkili olmayan kişilerin girişlerini engelleyecek şekilde tasarlanmıştır. Bu işlem 3 aşamada gerçekleştirilir[3].

- Kimlik belirleme (identification);

Bu aşamada kullanıcıya kendisini tanımlaması için özgün bir bilgi sorulur. Bu bilgi genellikle kullanıcı adı, e-posta adresi, kimlik numarası, yada hesap numarası olabilir.

- Kimlik doğrulama (Authentication);

Bu aşamada kullanıcı, tanımladığı kimliğin kendisine ait olduğunu ispatlamak için bir delil sunar. Bu delil, kullanıcının bildiği bir şifreyi girmesi, daha önceden belirlemiş olduğu bir varlığı giriş anında tekrar tanıması yada daha önceden gösterdiği bir davranışı sisteme giriş anında tekrar göstermesi gibi farklı yollarla sunulabilir.

- Yetkilendirme (Authorization);

Kimliğin kendisine ait olduğunu ispatlayan kişiye sistemde sahip olduğu yetkileri verme aşamasıdır.

Bu tezde alternatif bir kimlik doğrulama yöntemi sunulacaktır.

2.1 Kimlik Doğrulama

Güvenlik sistemlerinin kimlik kanıtlama mekanizması şu mantığa dayanır;

Kişilerle sistem arasında gizli bir bilgi tutulur ve sistem bu bilgiyi doğru olarak sağlayabilen kişinin doğru kişi olduğunu kabul ederek gerekli yetkilendirmeyi yapar. Burada bahsedilen gizli bilgi sisteme göre değişiklik gösterebilir. Kullanıcının ezberlediği ve biliyor olması gereken bir bilgi, kullanıcının ezberlemesi gerekmeyen ancak gördüğünde tanıması gereken bir varlığın bilgisi veya kullanıcının kişiliğine ait olan bir bilgi sistem ve kullanıcı arasında gizli bir bilgi olarak paylaşılabilir [3-5].

2.2 Güvenlik

Bu bölümde şifreleme sistemlerinin maruz kaldığı güvenlik tehditlerinden bahsedilecektir. Güvenlik tehditleri genel olarak iki başlık altında toplanabilir. Bunlar, tahmin etme (Guessing Attack) ve ele geçirme (Capture Attack) saldırılarıdır [6-7].

2.2.1 Tahmin Etme Saldırısı (Guessing Attack)

Bu saldırı tipinde saldırgan, şifrenin kullanıcı tarafından kolayca hatırlanabilecek parçalardan oluştuğunu varsayarak denemeler yapar. Metin tabanlı şifrelerde daha çok adı, soyadı, doğum tarihi gibi kişisel bilgiler tahminde kullanılır. Grafik şifrelerde ise kullanıcıların daha kolay hatırlayabilmek için örüntülü secimler yapmış olma olasılığı değerlendirilir. Grafik şifreler de, metin tabanlı şifreler gibi tahmine dayalı saldırı türüne acıktır. Tahmin etme saldırı türlerini aşağıdaki iki bölümde sunulmuştur.

2.2.1.1 Kaba Kuvvet Saldırısı (Brute-Force Attack)

Saldırgan gerçek bir kullanıcı gibi davranır ve verilen grafikte doğru şifreyi oluşturmak için gerekli secim işlemlerini yaparak sisteme giriş yapmaya çalışır. Sözlük saldırısından farkı, bu yöntemde olası şifrelerden oluşan bir sözlük kullanılmamasıdır; bunun yerine tüm şifre uzayı denenir. Grafik şifrelerdeki şifre uzayının genellikle metin tabanlı şifrelere göre daha büyük olması nedeniyle de grafik şifrelerin metin tabanlı şifrelere oranla bu saldırı türüne daha dayanıklı olduğu savunulmaktadır.

2.2.1.2 Sözlük Atak Saldırısı (Dictionary Attack)

Sözlük saldırısı yönteminde saldırgan program, deneme yanılma yoluyla kullanıcının şifresini bulmaya çalışır. Denemeler ise önceden tanımlanmış, olası şifrelerden oluşan sözlükler kullanılarak yapılır.

2.2.2 Ele Geçirme Saldırısı (Capture Attack)

Kullanıcının şifresini direk ele geçirebilmek için yapılan saldırı türleridir. Bunun için kimi zaman kullanıcıyı kandırarak bir şekilde şifresini elde etmek, kimi zaman da bazı casus yazılımlar kullanılarak maksada ulaşmaya çalışılır.

2.2.2.1 Yandan/Kenardan Bakma Saldırısı (Shoulder Surfing Attack)

Bu saldırı tipinde saldırgan, kullanıcının sisteme giriş yaptığı sırada kullanıcıyı izleyerek şifresini elde etmeye çalışır. Özellikle kalabalık ortamlarda saldırgan kullanıcıya ve ekrana daha yakın durarak kullanıcının sisteme giriş sırasında yaptıklarını gözleyebilmektedir. Hem metin tabanlı şifre sistemleri hem de grafik tabanlı şifre sistemleri bu yönteme karşı savunmasızdır. Hatırlamaya dayalı ve ipucuyla geri çağırmaya dayalı bazı yöntemler bu saldırı tipine karşı dayanıklı hale getirilebilir. Tanımaya dayalı yöntemler ise bu saldırıya tamamen acıktır.

2.2.2.2 Casus Yazılımlar (Malware)

Casus yazılımlar kullanıcının izni ve bilgisi olmadan bilgisayara yüklenir ve arka planda çalışarak kullanıcının kişisel ve özel bilgilerini toplar. Grafik şifreler genel olarak resimdeki belirli bölgelerin belirli bir sırada seçilmesiyle oluşturulduğundan, arka planda casus yazılımlar çalışsa dahi kullanıcın şifresiyle oturum açarken seçtiği bölgeler ekran çözünürlüğüne bağlı olarak değişeceği için, grafik şifrelerin metin tabanlı şifrelere oranla bu saldırı tipine karşı daha dayanıklı olduğu savunulur.

2.2.2.3 Yemleme Saldırısı (Phishing Attack)

Yemleme genelde bir kişinin şifresini veya kredi kartı ayrıntılarını öğrenmek amacıyla kullanılır. Bir banka veya resmi bir kurumdan geliyormuş gibi hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahte sitelere yönlendirilir. Phishing saldırıları için ‘Bankalar, Sosyal Paylaşım Siteleri, Mail Servisleri, Online Oyunlar vb. sahte web sayfaları hazırlanmaktır. Burada bilgisayar kullanıcısında özlük bilgileri, kart numarası, şifresi vb. istenir. E-posta ve sahte sitedeki talepleri dikkate alan kullanıcıların bilgileri çalınır.

Saldırgan kişiler özellikle bankalar, mail servisleri, alış-veriş siteleri, sosyal paylaşım ağları(Facebook, Twitter, MySpace vb.) gibi arkadaşlık ve anlık sohbet sistemleri,

online oyunlar gibi kullanıcı adı ve parola kullanılarak giriş yapılan sistemlerin bir kopyasını hazırlayarak ilk adımı atarlar. Saldırganlar ellerinde mevcut olan e-posta listelerine veya hedefledikleri kişilere gönderdikleri e-postalarla kurbanlarını hazırladıkları sahte sayfalara yönlendirirler. Kurbanların sahte sayfalara girerek istenen bilgileri paylaşmasıyla saldırı amacına ulaşmış olur.

2.2.2.4 Sosyal Mühendislik Saldırısı (Social Engineering)

Güvenlik sistemlerindeki en zayıf halkanın insan olduğu varsayımına dayanır. Saldırgan, insanların eğilimlerinden ve kişisel ilişkilerden faydalanarak gizli bilgilere erişmeye çalışır. Grafik şifreleri sözel olarak anlatmak metin tabanlı şifrelere göre daha zor olduğu için, grafik şifreler bu saldırı tipine daha dayanıklıdırlar.

2.3 Kullanışlılık

Metin tabanlı klasik parola (şifre) en iyi bilinen ve en yaygın kullanılan kimlik doğrulama yöntemidir [1,3]. Kullanıcılar şifrelerini genelde kolay hatırlayabilecekleri şekilde belirlerler (doğum tarihi, memleketi, tuttuğu takımı ya da bir arkadaşının ismi gibi). Hatırlanması kolay şifreler saldırganlar için de kırılması kolay şifrelerdir. Diğer taraftan rastgele karakterlerden oluşturulmuş ve belli sayıda karakter içeren (en az 8 karakter gibi) şifreler, güçlü ve kırılması daha zor şifrelerdir. Ancak bu şekilde belirlenen şifreler, hatırlanması zor olduğu için kullanıcılar tarafından çok da tercih edilmezler. Bazı sistemler bu tür güçlü şifrelerin kullanılmasını zorunlu kılmıştır. Fakat bu durumda da kullanıcılar kurallara uygun olarak belirledikleri güçlü şifreleri bir yere not ederek kullanırlar ve bu durum ayrı bir güvenlik tehlikesi olarak karşımıza çıkar. Yukarıda kısaca bir örnek vererek bahsettiğimiz güvenlik-kullanışlılık kısır döngüsünü kırmak tahmin edilenin ötesinde zor bir problemdir. Güvenlik sistemlerini bir bütün olarak düşünecek olursak; içinde barındırdığı süreçler, kurallar, algoritmalar, protokoller ve donanımsal faktörlerle birlikte, unutulmaması gereken bir diğer faktör de kullanıcıdır. Arka planda alınan bir dizi güvenlik önlemi, kullanıcının belirlediği tahmin edilmesi kolay bir şifreyle bütün değerini kaybedebilir. Bu noktada sistemlerin ihtiyacı güvenliğin kullanışlı olmasıdır. Önceki bir çalışmada kullanışlı güvenliğin tanımı şu şekilde yapılmıştır:

"Bir (güvenlik) yazılımı (donanımı, sistemi); o yazılımı kullanması beklenilen kişilerce

- *Güvenilir ve gerekli bulunuyorsa,*
- *Yapılması gerekenler doğru bir şekilde anlaşılıyor ve güvenli bir şekilde yapılabiliyorsa,*
- *Devamlı kullanımda yeteri kadar rahat ve sorunsuz kullanılabiliyorsa,*

bu yazılım (donanım, sistem) Kullanışlı Güvenlik (usable security) özelliğine sahiptir." [1]

2.4 Metin Tabanlı Şifreler

Metin tabanlı şifreler güvenlik zaafları ve bazı kullanım problemlerine rağmen halen yaygın bir şekilde kullanılan kimlik doğrulama yöntemidir. Yapılan bir çalışma İngiltere'deki firmaların %93'ünün personel ve müşterileri için metin tabanlı şifreleme yöntemini kullandığını ve her kullanıcının ortalama 3 farklı kullanıcı adı-şifre çiftini ezberlemek zorunda olduğunu ortaya koymuştur. İnternet kullanıcılarının bir diğer problemi de güvenlik sebebiyle farklı sistemler için farklı parolalar oluşturmak zorunda olmalarıdır. Yapılan bir araştırma İnternet kullanıcılarından sadece %19'unun her sitede farklı şifre kullandığı gerçeğini göstermiştir [6,8-9].
Kullanıcıların birçok sitede kullandıkları farklı kullanıcı adı ve şifreleri güvenli bir şekilde saklayabilen ve ihtiyaç olduğunda sunabilen, aynı zamanda kullanıcıdan aldıkları bilgileri o site için güvenli birer şifre haline getirip kullanıcıya sunan şifre yöneticisi yazılımları kullanışlılık problemine kısmen çözüm sunan sistemlerdir. Ayrıca bazı bellenir (mnemonic) kelime hafıza teknikleri de şifre hatırlamada yardımcı olarak önerilmiştir [9].

2.5 Grafik Tabanlı Şifreler

Metin tabanlı şifrelere alternatif olarak geliştirilen kimlik kanıtlama yöntemleri de bulunmaktadır ve grafik şifreler bu yöntemlerden bazılarıdır. Grafik şifre fikri ve tasarımı ilk olarak Greg E. Blonder tarafından ortaya atışmıştır [10-11,4].

Grafik şifreler, bazı grafiksel öğeler üzerinde yapılan işaretlemeleri, resimdeki herhangi bir noktayı ya da daha önce gördüğü bir resmi tekrar hatırlayabilmeyi paylaşılan gizli bilgi olarak kullanıp yetkilendirme yapabilen sistemlerdir.

"*Bir fotoğraf bin sözcüğe bedeldir*" genel kabul görmüş bir prensiptir. Yapılan bilişsel psikoloji çalışmaları insan hafızasının sözel ifadelerden çok görsel bilgileri daha kolay hatırlayabildiğini ya da tanıyabildiğini göstermiştir. Grafik tabanlı sistemler kullanıcının daha kolay hatırlayabileceği görsel öğeleri kullanarak farklı bir yaklaşım getirmişlerdir[12-13,3].

Bu başlık altında grafik şifre kategorilerinin tanımlarıyla birlikte farklı kategorilerde geliştirilmiş olan grafik şifrelere örnekler verilerek grafik şifreler hakkında daha net bir fikir vermek amaçlanmıştır. Oluşturulan farklı grafik şifreler 3 kategoride incelenebilir:

2.5.1 Hatırlamaya Dayalı Şifreler

Hatırlamaya dayalı grafik şifre yöntemlerinde kullanıcının bir defa seçtiği veya oluşturduğu (ya da sistem tarafından belirlenen) bir yapıyı, nesneyi veya aktiviteyi yeniden oluşturması veya gerçekleştirmesi beklenir. Bu kategori içerisinde verilebilecek güzel bir örnek Passpoints yöntemidir [14-15,6].

2.5.1.1 Passpoints

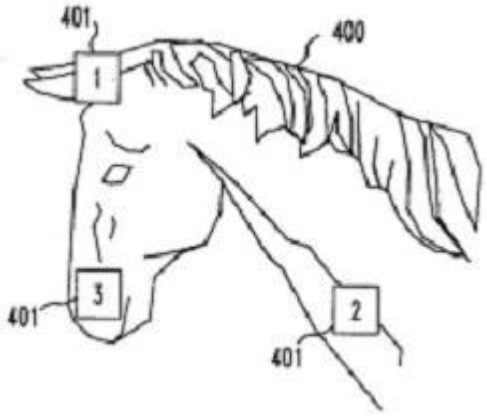
Passpoints yöntemi daha önce bahsedildiği üzere ilk defa ortaya atılan Blonder'ın grafik şifre yönteminden türetilmiştir. Passpoints'te Blonder'ın yönteminden farklı olarak önceden belirlenmiş alanlar bulunmamaktadır. Bu yöntemde kullanıcı resim üzerinde beş farklı noktayı fare ile tıklayarak seçer. Kullanıcının seçtiği bu noktalar o kişinin şifresi olarak belirlenmiş olur ve bundan sonraki girişlerde kullanıcı bu noktaları aynı sıra ile yeniden seçmelidir. Burada ilk defa seçilen nokta bir piksel olduğu için yeniden aynı tek pikseli seçmek çok zor olacaktır. Bu sebeple ilk başta tıklanılan pikselden belli bir uzaklıktaki piksellerin seçilmesini de kabul edilebilir görmek gereklidir. Bu yöntemde kullanılabilecek resim için bir sınır getirilmemekle birlikte bir resim üzerinde binlerce tıklanılabilecek alan bulunduğu için bu yöntemin şifre alanı oldukça geniştir. Bu yöntemde alfa nümerik şifrelere göre daha az denemede doğru şifrenin girilmesi gözlemlenmiştir ancak kullanıcıların şifrelerini

öğrenmeleri daha zor olmuş ve şifre girerken geçen süre artmıştır. Yine bu yöntemde karşılaşılan bir problem ise kullanılan resmin yapısından veya kullanıcıların yönelimlerinden kaynaklanan sebeplerle resim üzerindeki bazı noktaların diğer noktalara göre çok daha fazla seçilmesidir. Bu durum bir problem teşkil etmektedir çünkü bir saldırganın resim üzerinde yapacağı bir analizle belirlediği bazı noktalar üzerinde yoğunlaşıp dar bir şifre alanı üzerinde denemeler yapmasına imkân sağlamaktadır [16,17].

Şekil 2-1 PassPoints Grafik Şifreleme Yöntemi

2.5.1.2 Blonder

Bu yöntem fare ile tıklama tabanlı bir grafik parola yöntemidir. Kullanıcı verilen resimdeki önceden belirlenmiş seçilebilir bölgelerden istediklerini seçerek parolasını oluşturur.



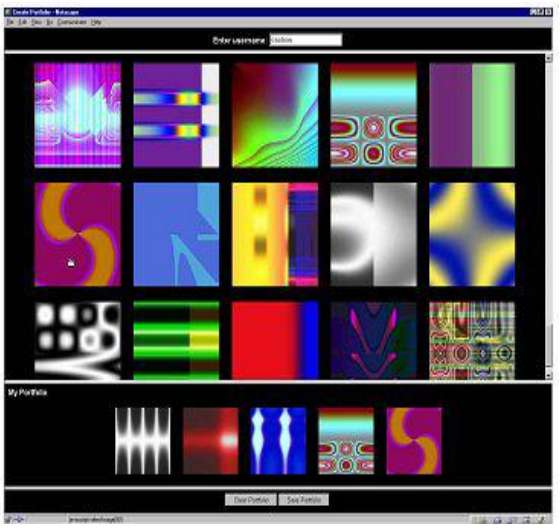
Şekil 2-2 Blonder Grafik Şifreleme Yöntemi [18]

2.5.2 Tanımaya Dayalı Şifreler

Tanımaya dayalı şifre yöntemlerinde kullanıcıdan bir resim kümesi içerisinden seçilen (veya sistemin belirlediği) bazı resimleri tıklaması beklenmektedir. Bu yöntemde kullanıcı birçok resim arasından bazı resimleri tanıyarak tıklamalıdır.
Real User Corporation tarafından geliştirilen Passfaces, tanımaya dayalı grafik şifre yöntemlerine örnek olarak verilebilir [10,11,19,3].

2.5.2.1 Déjà vu

Bu yöntemde kullanıcı kendisine sunulan çok sayıdaki resimden istediklerini seçerek parolasını oluşturur ve sisteme erişim sağlayabilmek için ilgisiz resimlerle birlikte sunulan resim kümesinden önceden seçtiği resimleri hatırlaması gerekir.



Şekil 2-3 Déjà vu Grafik Şifreleme Yöntemi

2.5.2.2 PassFaces

Passfaces de kullanıcıdan sunulan yüz resimleri arasından 4 tanesini seçmesi beklenmektedir ve seçilen bu resimler kullanıcının şifresi olarak belirlenmektedir. Sisteme giriş yapılacağı zaman Passfaces 8 adet çeldirici yüz resmi ve kullanıcının seçmiş olduğu yüzlerden 1 tanesini içerecek şekilde 9 adet yüz resmi gösterir. Kullanıcı sisteme girebilmek için bu resimlerden önceden seçmiş olduğu (ve dolayısıyla tanıyacağı) resmi seçmelidir. Bu işlem bu şekilde birkaç defa tekrar edilir ve eğer kullanıcı 4 resmi de doğru olarak seçmiş ise giriş işlemi gerçekleştirilir.

Bu yöntemin uzun vadede hatırlanabilir ve hata oranı düşük olduğu yapılan çalışmalarda görünse de güvenlik açısından eksikleri bulunmaktadır. Kullanıcıların bazı yüz resimlerine eğilimli olmaları sebebiyle (aynı ırktan veya güzel olduğu düşünülen yüz resimlerinin daha çok seçilmesi gibi) seçilen yüz resimlerinin tahmin edilebilir olması ve düşük şifre alanı gibi bazı güvenlik zayıflıkları bulunmaktadır [17].

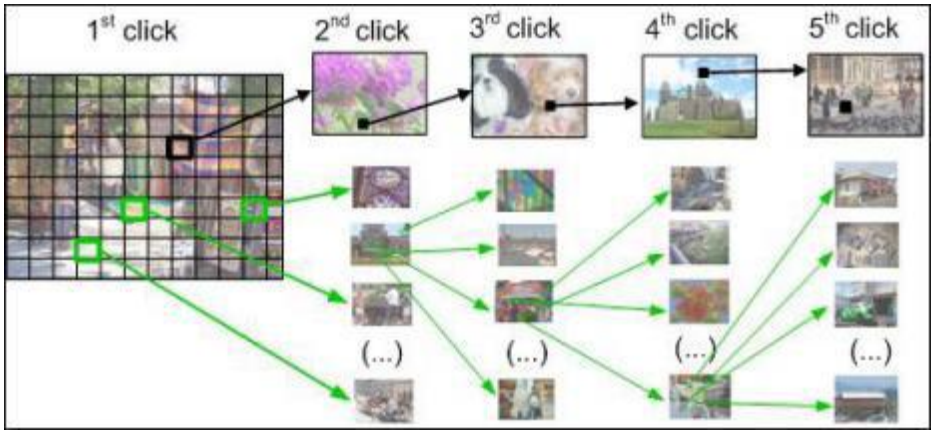
Şekil 2-4 PassFaces Grafik Şifreleme Yöntemi

2.5.3 İpucu ile Tanımaya Dayalı Şifreler

İpucuyla hatırlamaya dayanan yöntemler kullanıcının her bir tıklamasında tıklanılan şifrenin doğru olup olmadığı hakkında ipucu sağlayacak şekilde tasarlanmıştır [20,16,2].

2.5.3.1 Cued Click Points (CCP)

CCP, bu yönteme güzel bir örnektir ve PassPoints yöntemine benzerlik göstermekle birlikte birden fazla resim kullanmak gibi bazı farklılıkları da bulunmaktadır. Bu yöntemde kullanıcı her bir noktayı farklı bir resim üzerinden seçer. İlk resim üzerinde seçilen bir nokta kullanıcıyı diğer bir resme yönlendirir ve kullanıcı seçeceği diğer noktayı bu resim üzerinden seçer, bu işlem bütün noktalar (5 adet nokta) seçilene kadar tekrarlanır. Her bir resim bir önceki resimde tıklanılan noktaya göre gösterilir ve her bir nokta farklı bir resim gösterilmesini sağlar, bu şekilde kullanıcı şifresini tıklarken karşılaştığı resimlerden çıkarım yaparak doğru yolda olup olmadığı hakkında ipucu elde eder.



Şekil 2-5 Cued Click Points Grafik Şifreleme Yöntemi

2.6 Grafik ve Metin Tabanlı Şifre Yöntemlerinin Karşılaştırıldığı Çalışmalar

Bu bölümde grafik ve metin tabanlı yöntemlerin karşılaştırıldığı çalışmalara yer verilecektir [21].

İncelediğimiz ilk çalışma, Sacha Brostoff ve M. Angela Sasse tarafından yapılmıştır. Passface ile karakter tabanlı parolaların karşılaştırılması inceleniştir. Bu çalışmaya üniversite öğrencisi 34 kişi katılmıştır. Katılımcıların deney süresince Passface veya karakter tabanlı parolaları kullanma şekil şöyledir; her katılımcı dönem içinde aldıkları bir dersin ders notlarına ve/veya ödevlerine ulaşmak ve bunları sisteme uzaktan yüklemek için TACO [22] parola mekanizmasını kullanmaktadırlar. TACO' ya kimliklerini doğrulatmak için katılımcıların kendilerine dağıtılan bir ilk karakter parola ile sisteme girmeleri ve isterlerse daha sonra bu parolalarını değiştirmeleri sağlanmaktadır. 34 katılımcının yarısı deneyin ilk 5 haftasında sisteme girmek için ilk olarak karakter parolalarını ve sonraki adımda Passface parolalarını girmeleri istenmektedir. Diğer yarıyı oluşturan katılımcılar ise ilk olarak Passface parolalarını daha sonra karakter parolalarını girmeleri gerekmektedir. Deneyin son 5 haftasında yani kalan yarısında ise bu kullanıcı gruplarının parola girme yöntemleri birbiriyle değiştirilmiştir. Bu değişimi için katılımcıların sisteme yeniden kayıt edilmeleri için tekrar bir ilk parola bütün katılımcılara dağıtılmıştır.

Bu deney çerçevesinde oluşturulan Passface parolalarının entropi değerleri 12 bit olarak hesaplanmıştır, fakat karakter tabanlı parolalarında herhangi bir karakter

kümesi veya parola uzunluğu gibi bir sınırlama getirilmediği için karakter tabanlı parolaların entropi değerleri hesaplanamamıştır. Deney süresince veriler denek içi metodu ile toplanmıştır, her katılımcı her parola yöntemini kullanmıştır. Yeterli sayıda katılımcıya ulaşılamadığı için bu şekilde bir metodoloji izlenmiştir. Deney sonucunda toplanan verileri değerlendirirken, her katılımcının sisteme giriş yapmaktaki hata oranları şu şekilde hesaplanmıştır:

hatalı giriş sayısı / (hatalı giriş sayısı + başarılı giriş sayısı) (1)

Ve son olarak çıkarılan bütün sonuçların istatistiksel olarak anlamlı olup olmadıklarına karar vermek için ANOVA yöntemi kullanılmıştır.

Diğer bir çalışma, Rachna Dhamija ve Adrian Perrig tarafından geliştirilen Déjà Vu sistemi ile PIN ve karakter tabanlı yöntemler karşılaştırılmasıdır. [23] Déjà Vu, ilk olarak kullanıcılarından belli bir resim kümesinden kendileri için *n* sayıda resim seçerek bir alt küme oluşturmalarını istemektedir. Kullanıcıların sisteme kendilerini tanıtmaları için seçtikleri resimleri, herbirini sadece bir adımda, rastgele oluşan bir resim kümesi içinden tanımalarını istemektedir, bu tanıma süreci *n* defa tekrarlanmaktadır (seçilen her resim için bir defa).

Yürütülen deney çerçevesinde Déjà Vu (fotoğraflardan ve rastgele üretilen sanat resimlerinden oluşan) sistemleri ile karakter tabanlı parola ve PIN'ler karşılaştırılmıştır. Deneye 20 gönüllü katılımcı yardımı ile tamamlanmıştır. Her sistemin entropi değerleri ise şöyledir: Déjà Vu -fotoğraf- 16 bit, Déjà Vu -rastgele üretilen sanat resmi- 16 bit, karakter parola 14 bit ve son olarak PIN 13 bit'tir. Her katılımcı parolasını kendisi, Déjà Vu için kendi alt kümesini oluşturan resimleri veya fotoğrafları seçerek, PIN ve karakter parolası için istediği herhangi bir dizi girerek belirlemektedir. Deney bir hafta sürmüştür ve süreç boyunca katılımcılar 2 defa parolalarını kullanarak sisteme giriş yapmışlardır. Tablo 2.1'de görüldüğü gibi PIN ve karakter parolalar, Déjà Vu'ya göre zaman açısından daha iyi sonuçlara sahip olmalarına rağmen hatırlanabilirlik oranlarında özellikle bir hafta sonraki ikinci giriş için daha başarısız sonuçlandığı görülmüştür.

Son olarak incelediğimiz çalışma, Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle ve P. C. van Oorschot tarafından önerilen Persuasive Cued Click-Points (PCCP) [17] metodu ve bu metodun karakter tabanlı parolalara ile karşılaştırmasıdır. PCCP metodunun kullanımında, kullanıcılardan resim üzerinden bir nokta seçmelerini istemektedir fakat seçebilecekleri bu nokta resmin herhangi bir yerinden olmak yerine "görüntü kapısı" adı verilen 75x75 piksellik bir kısıtlı bir alan içerisinden olmak zorundadır.

Bu karşılaştırma için iki farklı deney uygulanmıştır, *field study* (kullanıcının evde,ofisde vb günlük kullanım alanlarında, ilgili yöntemi web ortamında kullanması, alan çalışması) ve *lab study* (kullanıcının laboratuarda yetkili bir kişi gözleminde ilgili yöntemi kullanması, laboratuar çalışması).

Laboratuar çalışması için katılımcılar her iki sistem içinde 6 farklı parolaya sahiptir. Katılımcılar ilk olarak her sistem için altı parolayı laboratuar da oluşturmuşlardır ve bundan iki hafta sonra tekrar laboratuara gelerek altı parolaları ile sisteme giriş yapmışlardır. Bu deney sonucunda PCCP'nin özellikle parola oluşturma aşaması karakter tabanlı parolalara göre çok uzun sürdüğü gözlenmiştir fakat hatırlanabilirlikleri ortalama aynı çıkmıştır. Laboratuar çalışması için karakter tabanlı parolalara 34 kişi, PCCP'ye 83 kişi gönüllü olarak katılmıştır. Web ortamında gerçekleştirilen alan çalışması ise 1 hafta sürmüştür ve katılımcılar bir hafta süresince 4 defa parolaları ile sisteme giriş yapmışlardır. Bu çalışma için her katılımcı 3 tane parolaya sahiptir. Çalışma sonucunda gözlemlenen sonuçlara göre PCCP'nin hatırlanabilirlik oranları karakter tabanlı parolalardan daha başarılı olduğu görülmüştür.

Çizelge 2.1 Grafik ve Metin Tabanlı Kimlik Doğrulama Yöntemlerinin Karşılaştırıldığı Tablo

Yöntemin İsmi		Çalışma Tipi	Tasarım	Entropi (bits)[1]	Şifre Belirleme Tipi	Kullanıcı Sayısı	Kullanıcı Başına Düşen Şifre	Oluşturma Zamanı (saniye)	İlk SistemeGiriş (saniye)	İkinciKere SistemeGiriş (saniye)	Birinci Başarı Oranı	İkinci Başarı Oranı
Story	Passwords	Alan çalışması n x 10hft[2]	Denek İçi	Bilinmiyor[3]	Kullanıcı Seçimi	34	Her kullanıcı için 1	Bilinmiyor	Bilinmiyor	Bilinmiyor	[4]	[4]
	Passfaces			12				Bilinmiyor	Bilinmiyor	Bilinmiyor	[4]	[4]
Déjà Vu	PIN	Laboratuar çalışması 2 x 1hft	Denek İçi	13/*	Kullanıcı Seçimi	20	Her kullanıcı için 1	15	15	27	95%	65%
	Passwords			14				25	18	24	95%	70%
	Art			16				45	32	36	100%	90%
	Photo			16				60	27	31	100%	95%
PCCP	Passwords	Laboratuar çalışması 2 x 2hft	Denekler Arası	52/18	Kullanıcı Seçimi	34	Her kullanıcı için 6	26	10	10	99%	31%
	PCCP			[5]	Sistem Ataması	83		91	18	27	99%	32%
PCCP (Web)	Passwords	Alan çalışması 4 x 1hft	Denekler Arası	36/14	Kullanıcı Seçimi	21	Her kullanıcı için 3	11	6	6	100%[6]	56%[6]
	PCCP			43	Sistem Ataması	24		68	13	20	99%[6]	67%[6]

[1] Teorik şifre alanı / NIST değerine göre.
[2] 10 hafta boyunca kullanıcılar ne zaman isterseler sisteme giriş yapabilirler
[3] En az şifre karakter limiti hakkında bir bilgi yok.
[4] 10 hafta boyunca süren deneyde birinci ve ikinci kez sisteme giriş başarı oranlarında herhangi bir bilgi not edilmemiştir.
[5] Katılımcılar rastgele bir 6 durumun birinden şifrelerini belirlemişlerdir. S5(küçük resim, 5 nokta, 43 bits, 14 katılımcı); S6 (küçük resim, 6 nokta, 53 bits, 14 katılımcı); S7(küçük resim, 7 noktas, 61 bits, 14 katılımcı); L5 (büyük resim, 5 resim, 52 bits, 14 katılımcı); L6 (büyük resim, 6 nokta, 63 bits, 12 katılımcı); and L7 (büyük resim, 7 nokta, 73 bits, 14 katılımcı). Küçük resmin boyutları 451x331 ve büyük resmin boyutları 800x600 pixel'dir. Görüntü kapısı ise 75x75 pixel'dir..
[6] Birinci ve ikinci sistem girişleri sırasında yöntemlerin başarı durumları arasında anlamlı bir fark olmadığı görülmüştür (PCCP Web and Metin Web).

2.7 Daha Önce Yapılmış Hibrit Kimlik Doğrulama Yöntemi

Grafik ve metin tabanlı kimlik doğrulama yöntemlerini önceki bölümlerde tanıtmış, birbirleriyle karşılaştırılması yapılan bazı çalışmaların sonuçlarını önceki bölümlerde sunmuştuk [24].

Bu bölümde, geliştirdiğimiz Yaz&Tıkla – ileri ki bölümlerde detaylı bir şekilde sunulacak - yönteminiyle aynı grupta değerlendirebileceğimiz, daha önce calışılmış hibrit yöntemlere yer vereceğiz.

Öncelikle P.C van Oorshot ve Tao Wan'ın birlikte tasarladığı "Two Step" isimli yöntem sunulacaktır.

Geliştirilen bu yöntem metin ve grafiksel öğeleri birlikte kullanmaktadır. Kullanıcı alışkanlıklarını çok fazla değiştirmeden metin tabanlı şifrelere grafiksel öğeleri de ekleyerek oluşturulan şifreyi tahmin edilmesi ve ele geçirilmesi daha zorlu bir hale getirebilmek amaçlanmıştır.

Kullanıcı şifresini 2 adımda oluşturmaktadır. Birinci adımda şifresinin metin kısmını oluşturmakta, ikinci adımda ise kendisine sunulan bir grup resimden bir yada daha fazla seçerek şifresini tamamlamaktadır. Kullanıcı her ne zaman sisteme giriş yapacak olsa şifresinin metin kısmıyla birlikte daha önce seçtiği resim yada resimleri de doğru bir şekilde hatırlamak zorundadır.

Bu yöntem sayesinde oluşturulan şifre, metin tabanlı yöntemlerin sıklıkla maruz kaldığı keylogger yada phishing attack gibi saldırılara karşı daha güçlü bir hal alır.

Ancak düşünülen bu yöntemin kullanıcı tarafından başarısını ölçebilecek herhangi bir deney henüz tasarlanmamıştır.

İncelediğimiz diğer çalışma ise Wazir Zada Khan, Yang Xiang, Mohammed Y. Aalsalem ve Quratulain Arshad'ın birlikte hazırladığı hibrit bir yöntemdir [25].

Yöntem daha çok akıllı cep telefonlarının dokunmatik özelliğinden faydalanarak kullanılmaktadır. Masaüstü bilgisayarlarda ise bilgisayar faresi yada touch pad sayesinde yöntem kullanılabilir.

Bu yöntemde kullanıcıdan, belirlediği kullanıcı adı ve metin şifresine ek olarak gösterilen objelerden en az üç tanesini, kullanıcıya gösterilen özel bir çerçeve içine eliyle çizmesi istenir. Çizilen bu üç obje bilgilerinden elde edilen kullanıcıya has el

hassasiyeti bilgileri bir takım algoritmalardan sırasıyla geçirilerek kullanıcıya özel bir bilgi elde edilir. Bu bilgi kullanıcının belirlediği kullanıcı adı ve metin şifreye atanır ve kullanıcı şifresi oluşturulmuş olur. Kullanıcı ne zaman sisteme giriş yapmak isterse girdiği kullanıcı adı ve metin şifresine ek olarak bu üç objeyi tekrar el ile çizmelidir. Kullanıcı eğer aynı hassasiyeti gösterebilirse sisteme giriş yapabilir. Bu durumda yöntemin yandan bakma saldırılarına karşı gücü görülmektedir. Saldırgan, kullanıcının hangi objeleri çizdiğini görse bile kullanıcıyla aynı hassasiyetle objeleri çizemeyeceğinden sisteme giriş yapamaz.

İncelediğimiz diğer çalışma ise Ayannuga Olanrewaju, Folorunso Olusegun ve Akinwale Adio tarafından geliştirilen hibrit yöntemdir [26].

Bu yöntemde kullanıcı, kullanıcı adını belirledikten sonra kendisine gösterilen küçük resimler kümesinden en az üç tanesini seçer. Daha sonra sistem kullanıcını yaptığı bu en az üç resme göre kullanıcıya 4 karakterlik bir metin şifresi belirler. Kullanıcı daha sonraki sistem girişlerinde kullanıcı adı, seçtiği en az üç resim ve sistemin kullanıcıya atadığı 4 karakterlik metin şifresini doğru bir şekilde girmek zorundadır.

Yapılan deneyin başarı sonuçları belirtilmemiş ancak yaklaşık 200 kişiye uyguladıkları yöntemi kullanıcılar genelde başarılı bulmuşlardır.

Bizim geliştirdiğimiz Yaz&Tıkla yöntemi de metin ve grafiksel öğeleri bir araya getiren hibrit bir yöntemdir. Ayrıca geliştirdiğimiz yöntemi laboratuar ortamında denenmiş olup, başarı sonuçlarını ilerleyen bölümlerde sunulacaktır. Bu anlamda, yapılan bu tez çalışması bilimsel literatürde deneysel olarak başarısı kanıtlanmış hibrit çalışma olarak yerini almıştır.

Konuyla ilgili yapılmış diğer çalışmalar belirtilen kaynak numarası ile sunulmuştur [30,31].

2.8 Şifre Alanı ve Entropi

Şifre uzayı, oluşturulması mümkün olan bütün şifrelerin kümesini oluşturur. Metin tabanlı şifrelerde 8 karakterli bir şifrenin içerisinde kullanılabilecek 26 küçük harf, 26 büyük harf, 10 rakam ve 32 özel karakter olduğunu varsayarsak, 94 farklı ASCII karakterden oluşturulabilecek şifre sayısı teorik olarak 94^8 olur. Ancak kullanıcılar kolay hatırlayabilmeleri için şifrelerinde rakam ya da özel karakteri kullanmak

istemezler ya da rastgele karakterler yerine anlamlı sözcükler tercih ederler. Dolayısıyla teoride mümkün olan şifre uzayına pratikte erişilemez. Benzer durum sıcak nokta probleminden ötürü grafik tabanlı şifrelerde de söz konusu olabilir. Fakat PCCP yönteminde sıcak nokta probleminin ihmal edilebilir seviyelerde kaldığı gözlemlenmiştir [27,6,7,17,16].

Belirsizliğin bir ölçütü olarak tanımlanan entropi, bilgi kuramında bilginin belirsizliği anlamına gelir. Şifreler bağlamında ise, belirlenen şifrenin belirsizliği ve dolayısıyla şifrenin gücünü nicel olarak ifade eden bir ölçüttür. Entropi değeri yukarıdaki örnekte yaklaşık $log_2(94^8) = 52,4$ bittir.

Şekil 2-6 Etkili Şifre Alanının İncelenmesi

2.9 Sıcak Nokta (Hot spot) Problemi

Metin tabanlı şifrelerde kullanıcıların hatırlamayı kolay kıldığı için kolay tahmin edilebilir şifreleri seçmeleri bilinen bir problemdir ve yukarıda da bahsedildiği üzere bu durum etkili şifre alanını düşürmektedir. Metin tabanlı şifrelerde bazı karakterlerin şifre elemanı olarak kullanılmamasının veya diğerlerine oranla çok az kullanılmasının sebebi bu karakterlerin uygun birer şifre elemanı olmamasıyla değil,

tamamen kullanıcı tercihleriyle ilgilidir. Grafik şifrelerde ise iki farklı sebepten dolayı bazı bileşenler çok az kullanılmakta veya hiç kullanılmamaktadır. Bu sebepler, tasarımdaki zayıflık ve kullanıcı tercihleridir [2,5].

Tasarım zayıflığı: Bir önceki başlıkta da örneklerle ifade edildiği gibi şifre tasarımının içerdiği bileşenlerden bazıları grafik şifre elemanı olmaya uygun aday 13 değilse (örneğin düzlükler gibi ayırt edici bir özellik içermiyorsa) kullanıcılar tarafından seçilmezler. Bu durum şifrelere karşı yapılacak olan saldırıyı kolaylaştırır.

Kullanıcı tercihleri: şifre tasarımındaki bileşenler homojen olarak dağıtılmış olsa ve her bir bileşen şifre elemanı olmaya uygun bile olsa kullanıcılar tarafından tercih edilmeyebilirler. Bunun sebeplerinin kullanıcılardaki eğilimler, bileşenlerin insanlar arasındaki popülerlik farkları, bileşenlerin görsel kalitesi gibi birçok sebep olması mümkündür.

Bir grafik şifre tasarımında kullanıcılar tarafından herhangi bir sebeple bazı bileşenlerin (noktaların, resimlerin, nesnelerin) diğerlerine göre seçilmesi daha muhtemel ise bu bileşenler sıcak noktalardır (Hot Spot).

Grafik şifreler arasında dikkat çeken bir çalışma olan PassPoints yönteminde tek bir arka plan resmi kullanılır ve sisteme giriş için resim üzerindeki 5 farklı noktanın (veya nokta merkez olmak üzere 19 x 19 piksellik bir karenin) doğru sırayla tıklanması gerekmektedir. PassPoints de kullanılan havuz resmi üzerinde yapılan bir güvenlik araştırmasına göre, sadece 15 kullanıcının en çok tıkladığı noktalar (sıcak-noktalar) tespit edilerek, bu noktaların oluşturabileceği tüm şifreler tespit edilmiş ve bir sözlük oluşturulmuştur. Bu sözlük kullanılarak 114 şifre içinden 30 adet şifre yani kullanıcı şifrelerinin %27 si başarıyla tahmin edilebilmiştir. Bu araştırma sıcak nokta probleminin göz ardı edilemeyecek kadar önemli bir problem olduğunu ortaya koymaktadır [2].

Sıcak nokta problemine bir çözüm önerisi olarak şifre seçimini kullanıcılara bırakmamak ve her kullanıcıya sistemin bir şifre ataması düşünülebilir fakat bu durumun şifre hatırlamada zorluk çıkarıp kullanışlılığı düşüreceği açıktır. Sistem atamalı şifrelerde hatırlama oranını dolayısıyla kullanışlılığı arttıracak bir yöntem bulunabilirse sıcak-nokta problemi kullanışlılığı düşürmeden tamamen ortadan kaldırılmış olur.

Grafik şifreler üzerine yapılan çalışmalar ve grafik şifrelerin problemlerinin tespitiyle birlikte çözüm önerileri sunulmaya ve incelenmeye devam ediyor. Grafik şifrelerin yeni bir kimlik kanıtlama sistemi olarak metin tabanlı şifrelere alternatif olması yapılan çalışmalar ve geliştirmelerle birlikte çok uzak görülmemektedir. Fakat geliştirilen grafik şifre yöntemi ne kadar güvenli ve kullanışlı olsa da bu sistemlerin kabul görmesi ve yaygınlaşması için aşılması gereken bir engel daha vardır. Bu engel kullanıcı alışkanlıklarıdır. İnsanların alışkanlıklarını değiştirmeleri ve yeni bir sisteme alışmaları zordur. Bu sebeple geçiş aşamasında insanları yeni grafik şifre sistemlerine mecbur bırakmak yerine kullanımda olan metin tabanlı sistemlerle bütünleşik olarak çalışabilecek bir gerçekleştirimin daha uygun olacağını düşünmekteyiz.

2.9.1 Görüntü Kapısı Teknolojisi (Persuasive Teknolojisi)

Görüntü kapısı, grafik tabanlı kimlik doğrulama yöntemlerinde ciddi bir problem oluşturan sıcak nokta problemini – önceki bölümde anlatılmıştır – aşmak ve kullanıcıları resim üzerinde tahmin edilmesi daha zor noktalara tıklamaya teşvik yada ikna etmek için Fogg tarafında geliştirilmiş bir teknolojidir [28].

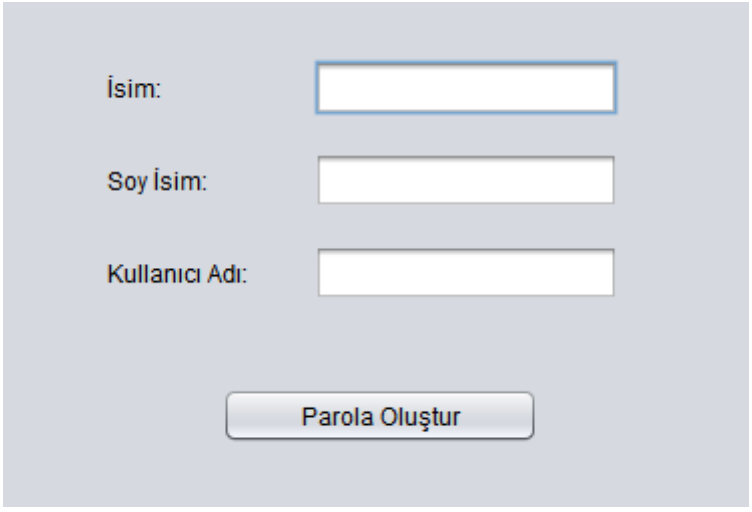
CCP (önceki bölümde anlatılmıştır) yönteminde resim üzerine tıklanılan bir nokta kullanıcıyı yeni bir resime yönlendirir, bu şekilde birkaç resim üzerinde tıklanılan noktalarla şifre oluşturulur. PCCP, (ileriki bölümlerde daha detaylı anlatılacak, ayrıca geliştirdiğimiz Yaz&Tıkla yöntemiyle karşılaştırılacak yöntemlerden bir tanesidir.) CCP yöntemine eklenen “Persuasive” teknolojisiyle oluşturulmuştur. Bu teknolojiyle kullanıcı resim üzerinde istediği noktaya değilde, sistemin kullanıcıya sunduğu resim üzerindeki bir görüntü kapısının içinde herhangi bir yeri tıklayabilir. Kullanıcı isterse sadece görüntü kapısının yerini değiştirebilir ancak görüntü kapısının yeni yeri resim üzerinde sistemin atadığı rastgele bir konumdur. Bu sayede resim üzerindeki sıcak noktalardan uzaklaşmış, rastgele bir noktayı şifrenin parçası olarak belirlemeye kullanıcı ikna edilmektedir. Görüntü kapısı teknolojisi PCCP yönteminde olduğu gibi Yaz&Tıkla yönteminde de kullanılmıştır. İlerleyen bölümlerde görüntü kapısının resim üzerindeki kullanımı şekillerle gösterilmiştir.

BÖLÜM 3 - KARŞILAŞTIRILACAK YÖNTEMLER

Bu çalışmada üç farklı kimlik doğrulama yöntemi deneysel olarak karşılaştırılmaktadır. Bu yöntemlerden birincisi metin tabanlı şifre yöntemi, ikincisi grafik tabanlı PCCP yöntemi ve üçüncüsü tarafımızca geliştirilen Yaz&Tıkla adlı melez şifre yöntemidir.

Kimlik tanıma yöntemleri arasında anlamlı bir karşılaştırma yapılabilmesi için her bir yöntem ile oluşturulacak şifrenin sağladığı güvenliğin eşit seviyede (eşit entropi değerine sahip) olması gerekir. Ayrıca kullanıcı her üç yöntemde de benzer aşamalardan geçerek şifresini oluşturmalıdır. Karşılaştırılan üç yöntemde de kullanıcılar sırasıyla,

1. İsim-soyisim girip, kullanıcı adı belirler.
2. Şifresini belirler.
3. Belirlediği şifresini tekrar girerek şifresini doğrular.



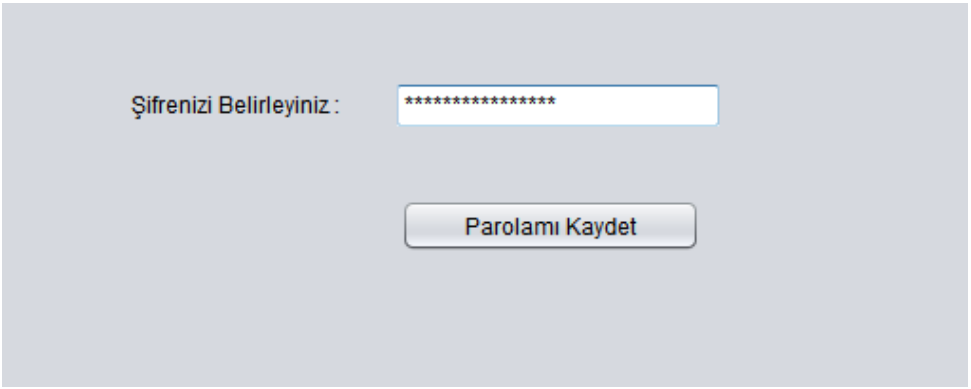
Şekil 3-1 Kullanıcı Bilgileri

Kullanıcıların her üç yöntemin başlangıcında kişisel bilgilerini girebildikleri sayfa, Şekil 3.1‘ de gösterilmiştir. Yöntemlerin şifre belirleme ve şifre doğrulama aşamaları, ilgili yöntemin anlatıldığı ilerleyen bölümlerde ayrıntılı bir şekilde anlatılacaktır.

Bu üç aşamayı da başarıyla gerçekleştiren kullanıcı (yukarıda numaralandırılmış aşamalar) ilgili yöntem ile kendine ait bir hesap oluşturmuş olur.

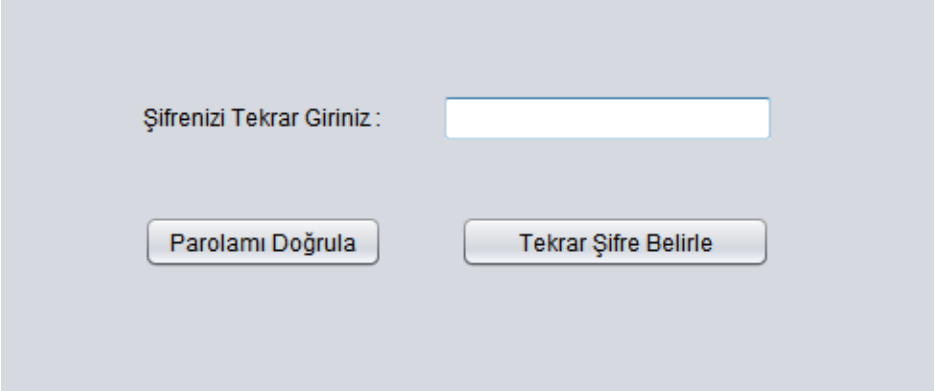
3.1 Metin Tabanlı Şifreler

Bu yöntem şifrenin sadece klavyeden girilen karakterler ile belirlenmesi prensibine dayanır. Kullanıcıdan şifresinde en az 14 karakter bulundurması istenmektedir. Bu tercihin sebebi 14 karakterden oluşan ve içinde herhangi bir özel karakter bulundurma zorunluluğu olmayan şifrenin entropi değerinin yaklaşık olarak 27 bit olarak tahmin edilmesidir (diğer iki yöntemde de belirlenen şifreler aynı entropi değerine sahiptir). Şekil 3.2'de kullanıcının bu yöntemde şifresini belirlerken karşılaştığı sayfa gösterilmiştir. Kullanıcı en az 14 karakter olarak belirlediği şifresini resim de gösterilen TextBox'a girer ve "Parolamı Kaydet" butonuna tıklayarak şifresini kaydeder ve bir sonraki şifre doğrulama aşamasına geçer.



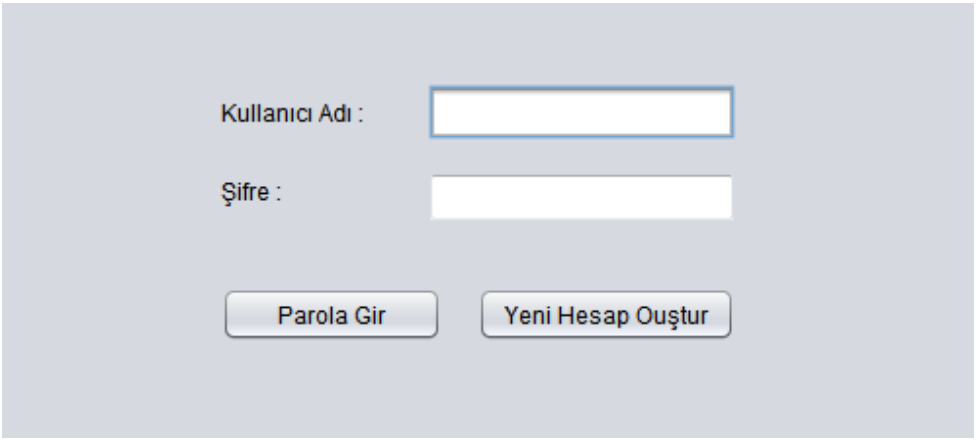
Şekil 3-2 Metin Tabanlı Yöntemde Şifre Belirleme

Şifre doğrulama aşamasında kullanıcının karşılaştığı sayfa Şekil 3.3'de gösterilmiştir. Bu aşamada kullanıcı bir önceki şifre belirleme aşamasında belirlediği şifresini tekrar giriş yaparak doğrular ve şifresini doğru belirlediğinden emin olur. Kullanıcı şifresini değiştirmek istediğinde "Tekrar Şifre Belirle" butonunu kullanarak bir önceki aşamaya dönüp şifresin değiştirebilir.



Şekil 3-3 Metin Tabanlı Yöntemde Şifre Doğrulama

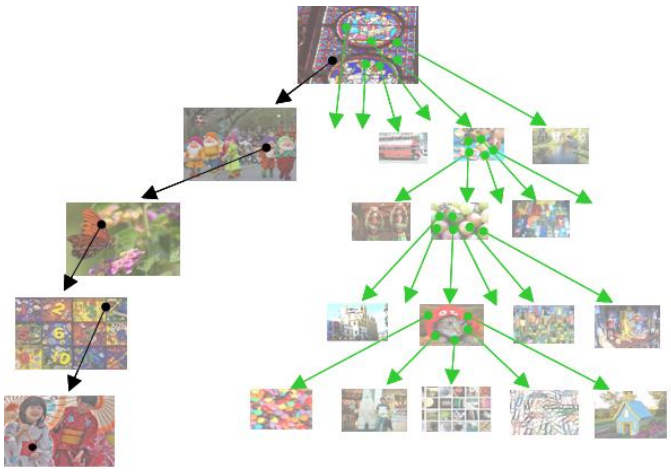
Şifresini başarıyla belirleyip kendisini sisteme kaydedebilen kullanıcılar Şekil 3.4'de gösterilen, metin tabanlı yöntem için sistem giriş sayfasını kullanarak sisteme giriş yapabilirler.



Şekil 3-4 Metin Tabanlı Yöntemde Sistem Girişi

3.2 PCCP (Persuasive Cued-Click Points)

PCCP, grafik tabanlı kimlik yönteminde kullanıcı art arda gelen resimler üzerinde birer kez tıklayarak şifresini oluşturur (Şekil 3.5).



Şekil 3-5 PCCP Grafik Tabanlı Yöntemin Mimarisi[20]

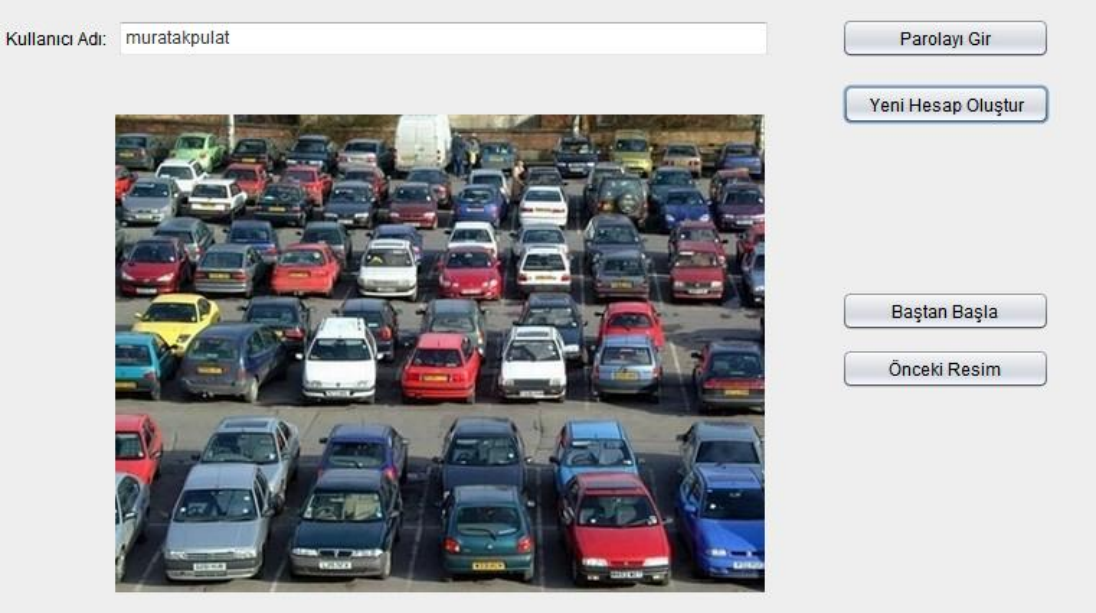
Kullanıcının kişisel bilgilerini girdikten sonra PCCP yönteminde şifresini belirlemek için geldiği sayfa Şekil 3-6'da gösterilmiştir. 451x331 piksel büyüklüğündeki resim üzerinde bulunan 75x75 piksel büyüklüğündeki görüntü kapısı (viewport) içinde kalan kısımdan bir yere tıklayarak parolasının her bir bileşeni oluşturulur. Kullanıcı "Değiştir" düğmesine basarak isterse görüntü kapısının yerini değiştirebilir. Ancak görüntü kapısının yeni konumu yine sistemin resim üzerinde rastgele belirlediği başka bir konumdur. Deneyde kullandığımız PCCP uygulamasında kullanıcıların 3 resim üzerinde tıklama yapması gerekmektedir. Eğer kullanıcı daha önceki adımlarda seçmiş olduğu resim ve/veya noktalardan vazgeçmek isterse "Baştan Başla" düğmesine basarak parola oluşturmaya tekrar baştan başlayabilir. Yada bütün işlemlere tekrar başlamak isterse bunu "Ana Ekrana Dön" düğmesine basarak gerçekleştirebilir.

Şekil 3-6 PCCP Grafik Tabanlı Yöntemde Şifre Belirleme

Şifre doğrulaması için kullanıcıdan bir önceki adımda oluşturduğu şifresini tekrar girmeleri istenecektir.(Şekil 3-7) Fakat bu sefer resimlerin üzerinde görüntü kapısı olmayacaktır. Kullanıcı şifre oluşturma aşamasında belirlediği noktalara tekrar tıklamak zorundadır. Eğer tıkladığı nokta bir önceki adımda şifresini oluştururken tıkladığı noktanın 19x19 piksellik bir tolerans aralığında değil ise karşısına şifre oluştururken kullandığı resimden farklı bir resim gelecektir. Bu durumda kullanıcının yanlış yere tıkladığını fark etmesi beklenir. Kullanıcı isterse "Önceki Resim" düğmesine basarak bir önceki resme dönebilir ya da "Baştan Başla" düğmesine basarak şifresini doğrulamaya en baştan başlayabilir.

Şekil 3-7 PCCP Grafik Tabanlı Yöntemde Şifre Doğrulama

Şifresini başarıyla belirleyip kendisini sisteme kaydedebilen kullanıcılar Şekil 3-8'de gösterilen sayfa üzerinde sisteme giriş yapabileceklerdir. Sistem girişi sayfasında "Kullanıcı Adı" ile istenen kısma kişisel bilgilerini girdiği sırada belirlediği kullanıcı adını yazdığı esnada dinamik olarak şifre belirleme aşamalarında gösterilen birinci resim ekrana gelecektir.



Şekil 3-8 PCCP Grafik Tabanlı Yöntemde Sistem Girişi

451x331 piksel resim boyutu, 19x19 piksel tolerans değeri ve 3 tıklama işlemiyle oluşturulan şifrenin entropi değeri aşağıdaki formülle bulunabilir.

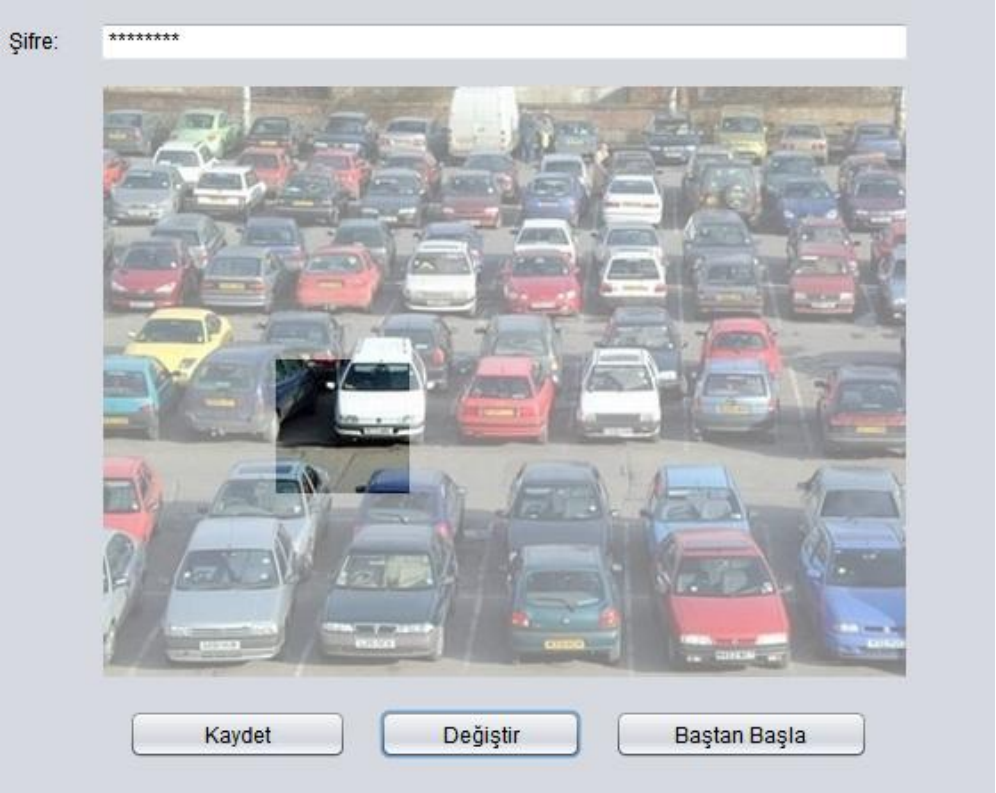
$$[\frac{451x331}{19^2}]^3 \cong 2^{27} \qquad (2)$$

Bu sonuca göre PCCP yönteminden de oluşan şifrenin entropi değeri 27 bit'tir.

3.3 Alternatif Geliştirilen Yöntem (Yaz&tıkla)

Tarafımızca geliştirilen bu yöntemde kullanıcının belirlediği metin tabanlı şifresine ek olarak bu şifreye bağıntılı olarak karşısına gelen bir resimde tek bir noktaya tıklaması istenir.

Kullanıcı şifresini belirleyebilmek için şifre oluşturma sayfasına gelir(Şekil 3-9). Bu sayfada kullanıcının şifresinin ilk kısmını oluşturabilmesi için bir metin giriş alanı ve girilen şifreye bağlı olarak dinamik olarak değişen bir resim vardır.



Şekil 3-9 Yaz&Tıkla Yönteminde Şifre Belirleme

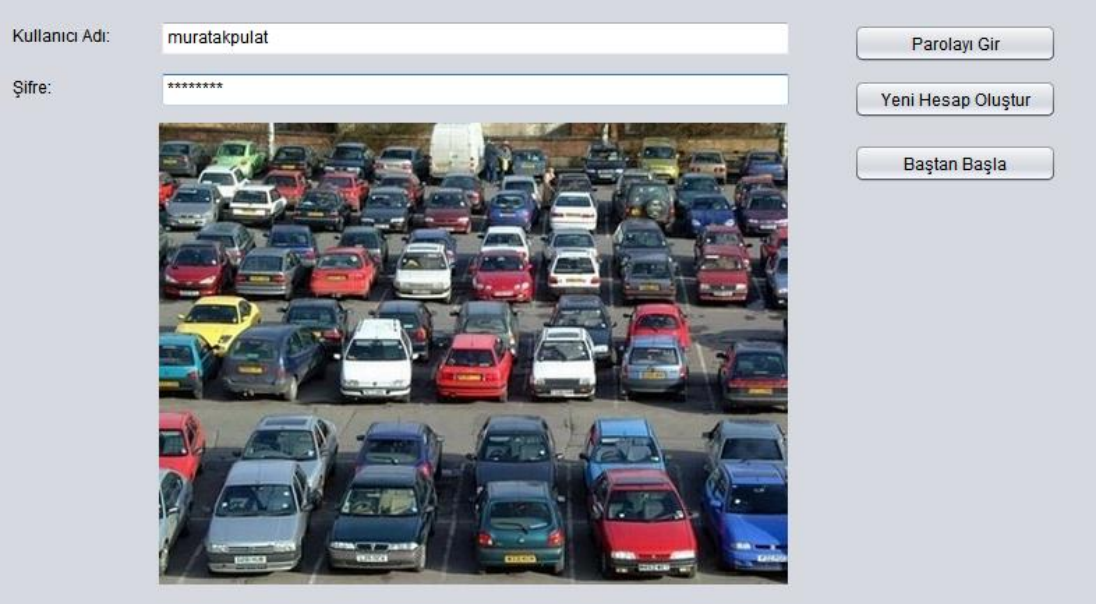
Kullanıcı metin giriş kısmına en az 8 karakterlik bir şifre girer. Belirlenen bu şifreye göre sistem kullanıcıya bir resim (451x331 piksel) gösterir ve resimde görüntü kapısı sınırları (75x75 piksel) içinde olmak koşulu ile bir tek noktaya tıklanması istenir. Sistem görüntü kapısının haricinde tıklanılan noktayı şifre olarak kabul etmez. Ancak PCCP' ye benzer şekilde "Değiştir" düğmesiyle kullanıcı eğer isterse bu sınırın yerini sistemin atadığı rastgele başka bir yere taşıyabilir. Kullanıcı tıklama işlemini gerçekleştirdikten sonra resmin artık tıklanılamaz olduğunu görür, artık şifrenin iki kısmı da belirlenmiştir. Ancak kullanıcı herhangi bir değişiklik yapmak istediğinde "Baştan Başla" düğmesine tıklayarak resmi tekrar aktif hale getirebilir, tıklanılan nokta ve şifrenin metin kısmında istediği değişikliği gerçekleştirebilir. Şifresini belirleyen kullanıcı, "Parolamı Kaydet" düğmesine tıklayarak belirlediği şifreyi doğrulamak üzere bir sonraki aşamaya ulaşır.

Şekil 3-10 Yaz&Tıkla Yönteminde Şifre Doğrulama

Şifre kısmına girilen her bir karakterle dinamik olarak ekranda değişen resmin sisteme her giriş yapıldığında aynı şekilde gösterilmesini sağlayan algoritma şu şekilde çalışır:

1. Kullanıcı adı ve şifrenin metin kısmı MD5 özet algoritmasından geçirilerek 128 bit veri elde edilir.
2. Verinin ilk 10 biti alınır.
3. 10 bitlik veri onluk tamsayıya dönüştürülür.
4. Bu tamsayı kullanıcıya gösterilen resmin indeks numarasıdır.

Sistem kullanıcı adının birden fazla kullanılmasına izin vermediği için kullanıcıların belirlediği şifreler aynı olsa bile görüntülenen resim farklı olur. Bu işlem aşamaları her karakter girişinde tekrarlanır.



Şekil 3-11 Yaz&Tıkla Yönteminde Sistem Girişi

Şifre doğrulamada kullanıcıdan belirlediği şifrenin metin ve tıklama aşamalarını doğru bir şekilde tekrarlaması istenir. Kullanıcı metin kısmına girdiği aynı şifreyle beliren aynı resimde 19x19 piksellik tolerans aralığında daha önce tıkladığı noktaya tekrar tıklar. Doğrulamada resim üzerinde görüntü kapısı yoktur.

Şifrenin metin kısmı girilirken resmin dinamik olarak değişmesi kullanıcıya hemen o anda şifre doğrulama imkânı sunar. Kullanıcı eğer şifresini girdiğinde beklediği resimle karşılaşmazsa şifresini yanlış girdiğini anlayabilir. Yani resim kullanıcı için şifrenin her karakteri için bir ipucu olur (fakat söz konusu bu geri besleme başkaları için bir ipucu teşkil etmez). Çünkü kullanıcı şifrenin her karakterini sırasıyla girdiğinde sistemin gösterdiği resim sırası hep aynıdır. Böylece kullanıcı şifrenin hangi karakterinde hata yaptığını dahi anlayabilir.

Bu yöntemle oluşacak şifrelerin entropi değerleri metin ve resim kısımlarının entropi değerleri ayrı ayrı belirlenerek bulunabilir. Sadece en az sekiz karakter bulundurma zorunluluğu olan metin kısmın entropiye katkısı yaklaşık 18 bittir. Resim üzerine tek tıklamayla elde edilen entropi değeri de yaklaşık 9 bittir. Böylece toplamda bu yöntemle oluşturulan şifrelerin entropi değeri de 27 bit olarak bulunur.

BÖLÜM 4 - METODOLOJİ

İlk olarak deneysel olarak test edilecek hipotezler belirlenmiştir. Bu hipotezler;

1- Yaz&Tıkla yöntemi ile belirlenen şifreler diğer iki yöntem ile belirlenen aynı güvenlik seviyesindeki şifrelere göre uzun vadede kullanıcılar tarafından daha iyi hatırlanacaktır.
2- Kullanıcılar Yaz&Tıkla yöntemi ile oluşturulan şifreleri diğerlerine nazaran daha güvenli ve daha kullanışlı olarak algılayacaktır (bir sistemin güvenli olması kadar kullanıcılar tarafından da güvenli bulunması o sistemin pratikte uygulanabilirliği açısından çok önemlidir).
3- Kullanıcı Yaz&Tıkla yöntemi ile oluşturduğu birden fazla şifreyi yaklaşık başarı oranı ile hatırlayacaktır.

Aşağıda, belirlenen hipotezleri test etmek için tasarlanan deneyde takip edilecek metodoloji kısaca tanıtılmaktadır.
İki deneyden oluşan laboratuar çalışmamız Kelkit Aydın Doğan Meslek Yüksekokulu Bilgisayar Teknolojileri bölümü öğrencilerinden 76 (1. sınıf 10 bayan- 16 bay yaş ortalamaları 21.1 , 2. sınıf 19 bayan- 31 bay yaş ortalamaları 22.3) kişinin katılımı ile gerçekleştirilmiştir. Kullanıcıların tamamı e-posta, alış-veriş, vb. şifre gerektiren siteleri aktif olarak kullanabilmektedirler.

4.1 Birinci Deney

Deneyin birinci bölümü iki aşamadan oluşmaktadır. İlk aşamada kullanıcılar 6-7'li gruplar halinde laboratuara davet edilmişler ve sistem hakkında 5 dakika süresince aşağıdaki konularda bilgilendirilmişlerdir:

1- Deneyin amacı (hangi sistemin tarafımızca geliştirildiği açıklanmamıştır).
2- Sistemin doğru sonuçlar verebilmesi için daha önce kullanmadıkları ve ezberlerinde olmayan bir şifre kullanmaları,

3- Önemli bilgilerinin bulunduğu bir e-posta hesabının yada banka hesabının şifresini belirleyeceklerini düşünerek bu sistemi kullanmaları,
4- Belirledikleri şifreleri herhangi bir yere not etmemeleri,
5- Metin ve Yaz&Tıkla yöntemlerindeki şifrelerinin metin kısımlarının benzer olmaması gereği.

Daha sonra kullanıcılar yaklaşık 10 dakika boyunca programı denemiş ve kullanımına alışmışlardır.

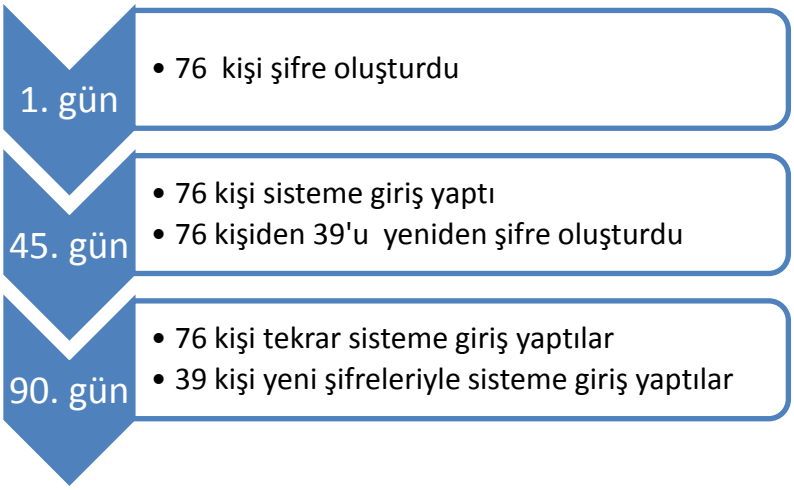
İlk aşamanın son adımı olarak her kullanıcıdan her üç yöntem ile de sisteme giriş yapmaları istenmiştir (Denek-İçi (Within-Subjects) metodu kullanılmıştır). Dolayısıyla her kullanıcı 3 farklı şifre oluşturmuş ve onaylamıştır. Yöntemlerin kullanılma sırası kullanıcıların isteklerine bırakılmıştır. Kullanıcılara 45 gün sonra sisteme 3 yöntem ile de giriş yapmak için tekrar davet edilecekleri söylenerek ilk aşama tamamlanmıştır. İkinci aşama 45 gün sonra gerçekleştirilmiş ve kullanıcılardan ilk aşamada belirledikleri şifreler ile sisteme tekrar giriş yapmaları istenmiştir. Sistem girişlerinden hemen sonra yapılan anket çalışması ile ikinci aşama sonlanmıştır.

4.2 İkinci Deney

Bu bölümde birinci bölümü tamamlamış 76 kullanıcıdan 39'unun yeniden şifre belirlemesini istedik. Bu 39 kullanıcı yine farklı zamanlarda 6-7'li gruplar halinde laboratuara davet edilip yeni şifrelerini belirlemişlerdir. Kullanıcılar önceki bölümü gerçekleştirdiklerinden programın kullanımı ve dikkat edilmesi gereken hususlar hakkında bilgi sahibidirler. Ancak bu sefer kullanıcılardan istenen, daha önce oluşturdukları şifrelerden tamamen farklı şifreler oluşturmalarıdır (kullanıcı adının farklı olması noktasında herhangi bir uyarıda bulunulmamıştır.). Artık kullanıcıların 76'sından 39'unun her yöntemden oluşturdukları 2 şer adet şifreleri bulunmaktadır.

Bu bölümün son aşaması 45 gün sonra gerçekleştirilmiştir. 39 kullanıcı laboratuara davet edilmiş ve oluşturdukları eski ve yeni şifreleri ile tekrar sisteme giriş yapmaları istenmiştir.

Bu bölümde aşamaları anlatılan deneylerin grafik üzerinde gösterimi Şekil 4-1 ‘de sunulmuştur.



Şekil 4-1Deney Aşamalarının Grafik Üzerinde Gösterimi

BÖLÜM 5 - SONUÇLAR

Deney süresince toplanan veriler ışığında ulaşılan sonuçlar aşağıda özetlenmiştir. Deneylerde kullanıcıların sisteme giriş işleminde ne kadar başarılı olabildikleri ve bu başarıyı ne kadarlık süre zarfında gösterebildikleri ölçülmektedir.

5.1 Başarı Oranları

Metodolojide laboratuar çalışmasının iki deneyden oluştuğu ve bu deneylerde yapılması gereken işlevlerden bahsedilmişti. Bu bölümde ise kullanıcıların sisteme başarılı giriş sayılarından elde edilen sonuçlar sunulacaktır.

5.1.1 Birinci Deneyin Başarı Sonuçları

Bu deneyde kullanıcıların yöntemleri kullanırken gösterdikleri başarı oranları sunulmuştur. Başarı oranları iki farklı durum için incelenmiştir:

1- Kullanıcının şifresini belirlerken ilk aşamada gösterdiği başarı.
2- Kullanıcının 45 gün sonra ikinci aşamada gösterdiği başarı.

Tablo 5-1'de PCCP ve Yaz&Tıkla yöntemlerinde başarı oranları sunulurken şu şekilde bir ayrım yapılmıştır. Kullanıcılar "Baştan Başla" ve "Önceki Resim" düğmelerine tıklamadan parolasını girebilmiş (ve ilk aşamada doğrulayabilmiş) ise "Başarılı", eğer bu düğmelere basarak parolasını girebilmiş (ve doğrulayabilmiş) ise "Düzelterek Başarılı" addedilmiştir.
Üç yöntemde de parolasını önce hatalı sonra doğru girenler yine "Düzelterek Başarılı" kategorisinde değerlendirilmiştir. Tablo 5-3'de Düzelterek Başarılı ve Başarılı sonuçları "Başarılı" başlığı altında birleştirilerek ikinci aşamada elde edilen sonuçlar tekrar özet bir şekilde sunulmuştur. Tablo 5-3'de görüleceği üzere Yaz&Tıkla yöntemi % 80'i aşan oranı ile diğer iki yöntemden daha fazla başarılı olmuştur. Bu başarı sonuçları ışığında birinci hipotezimizin doğru olduğuna dair bir delil elde edildiği - Yaz&Tıkla yöntemi ile oluşturulan şifrelerin kullanıcılar için daha hatırda kalır olduğu - sonucuna varabiliriz. Bu başarı oranları istatistiksel

anlamlılık bağlamında incelendiğinde aralarında anlamlı bir fark olduğu görülmektedir.[F(2-225)=3.82,p<0.023]

Deney esnasında yaptığımız gözlemler bizde şu fikri oluşturmuştur. Kullanıcıların PCCP yöntemindeki şifrelerinin tamamen resim üzerinden belirlemeleri grafik tabanlı şifrelere aşina olunmadığı için kullanışlılık problemi oluşturmuştur. Yaz&Tıkla yönteminde ise ilk başta metin şifre girilmesi ve sonrasında tek resimde tıklama işlemi uygulanması kullanıcıların sisteme daha kolay adapte olmasını sağlamıştır.

Çizelge 5.1 Yöntemlerin Başarı Oranları

	Parola Girme		**Parola Girme (45 gün sonra)**		
	Başarılı	**Düzelterek Başardı**	**Başarılı**	**Düzelterek Başardı**	**Başarısız**
PCCP	76/76	28/76	48/76	25/76	28/76
	%100	%36,84	%63,16	%32,89	%36,84
Yaz&Tıkla	76/76	14/76	63/76	14/76	13/76
	%100	%18,42	%82,89	%18,42	%17,11
Metin	76/76	18/76	55/76	20/76	21/76
	%100	%23,68	%72,37	%26,32	%27,63

Çizelge 5.2 Yöntemlerin Sınıflara Göre Gruplanmış Başarı Oranları

	1. sınıf (26 kişi)			**2. sınıf (50 kişi)**		
	Başarılı	**Düzelterek Başardı**	**Başarısız**	**Başarılı**	**Düzelterek Başardı**	**Başarısız**
PCCP	14/26	11/26	12/26	34/50	14/50	16/50
	%53,85	%42,31	%46,15	%68	%28	%32
Yaz&Tıkla	20/26	6/26	6/26	43/50	8/50	7/50
	%76,92	%23,08	%23,08	%86	%16	%14
Metin	15/26	10/26	11/26	40/50	10/50	10/50
	%57,69	%38,46	%42,31	%80	%20	%20

Çizelge 5.3 Başarı Oranları Özet Tablosu

	Parola Girme(45 gün sonra,76 kişi)		
	Başarılı	**Başarısız**	**Başarı Oranı %**
PCCP	48	28	63,16
Yaz&Tıkla	63	13	82,89
Metin	55	21	72,37

Çizelge 5.4 Yöntemlerin Sınıflara Göre Gruplanmış Özet Başarı Tablosu

	1.sınıf		2.sınıf	
	Başarılı	**Başarısız**	**Başarılı**	**Başarısız**
PCCP	%18,42	%15,79	%44,74	%21,05
Yaz&Tıkla	%26,32	%7,89	%56,58	%9,21
Metin	%19,74	%14,47	%52,63	%13,16

Çizelge 5.5 Resim Üzerindeki "Görüntü Kapısı" nın yerini değiştirme sayısı

	PCCP			Yaz&Tıkla
	Resim 1	**Resim 2**	**Resim 3**	**Resim 1**
Ortalama	13,7	9,1	7,6	15,3
Ortanca	5,00	5,00	4,00	9,00

45 gün sonra tekrar sisteme giriş yapılması esnasında kullanıcılardan birçoğunun Yaz&Tıkla yöntemini kullanırken ekranda görünen resimler yardımı ile şifrelerinin metin kısmının doğruluğunu kontrol ettikleri gözlemlenmiştir.

Kullanıcının, şifresinin ilk kısmını hatırlar ve doğru resme ulaşırsa, resimde yaptığı tıklamada çok da zorlanmadığı görülmüştür. Bazı kullanıcılar Yaz&Tıkla yöntemini kullanırken şifresinin metin bölümünü belirlerken görünen resme göre metini değiştirmiş ve kendisi için kolay olabileceğini düşündüğü resme karşılık gelen metini şifrenin ilk kısmı olarak belirlemiştir. Aslında benzer bir durum PCCP'de de vardır. Ancak kullanıcıların resimler üzerinde tıklama işlemlerini birkaç defa denemesi ve beğenmediği resmi değiştirmek için önceki resme dönüp tekrar nokta belirlemesi

kimi zaman konsantrasyon kaybına ve hatalara sebep olduğu gözlemlenmiştir. Kullanıcıların görüntü kapısını tolerans aralığı olarak algılaması ve ona göre şifre doğrulama işlemleri yapması iki yöntemde de (PCCP ve Yaz&Tıkla) karşılaşılan bir diğer problemdir. Metin tabanlı yöntemde en az 14 karakterden oluşan şifreleri 45 gün sonra hatırlamak yaklaşık kullanıcıların yarısı için mümkün olmamıştır. Kullanıcıların bazılarının kısa cümlecikleri şifre olarak belirlemeleri sayesinde başarılı oldukları gözlemlenmiştir (örnek: şampiyonfenerbahçe).

Tablo 5-5'de PCCP ve Yaz&Tıkla yönteminde "değiştir" düğmesini kullanma sayısı yani resim üzerindeki "görüntü kapısı" nın yerini değiştirme sayıları verilmiştir. Bu sayıların resim başına ortalamada yaklaşık aynı olması güvenlik (sıcak nokta problemi) konusunda bu iki yöntemin yaklaşık aynı özellikleri gösterdikleri konusunda bir ipucu teşkil etmektedir.

Bu değerleri 1. ve 2. sınıflara göre gruplandırıp incelediğimiz elde ettiğimiz başarı durumu başarı durumları tablo 5-2' de ve özet haliyle tablo 5-4 'de sunulmuştur. Sonuçlar 2. sınıfdaki kullanıcıların 1. sınıfdaki kullanıcılara göre ortalama iki kat daha fazla başarılı olduğunu göstermektedir. Bu sonuçlara göre bilgisayar kullanım alışkanlığının bu ve benzeri sistemleri başarıyla kullanım noktasında nedenli etkili olduğunu göstermektedir.

5.1.2 İkinci Deneyin Başarı Sonuçları

76 kullanıcının 39'u üzerinde gerçekleştirilen ikinci deneyde, her yöntemden 2 şer adet şifreye sahip olan kullanıcılar 45 gün aradan sonra sisteme tekrar giriş yapmışlardır. Bu durumda kullanıcılar birinci şifrelerini 90 gün sonrasında, ikinci şifrelerini ise 45 gün sonrasında sisteme giriş yapmak için kullanmışlardır. Bu işlemler sonunda elde edilen başarı oranları tablo 5-6'da sunulmaktadır. Bu sonuçlara göre kullanıcıların 90 gün sonunda 1. parolalarının sisteme girişinden elde ettikleri %70'i aşkın başarıyı, 45 gün sonraki 2. parolalarında da göstermişlerdir. Ancak bu seferki sonuçlar istatistikî değerlendirme bakımından diğer yöntemlerle karşılaştırıldığında anlamlı çıkmamıştır. [$F(2\text{-}114)=1.447, p>0.05$]. Yaz&Tıkla ve Metin tabanlı yöntemlerinin başarı oranlarının birbirine yakın olduğu görülmüştür.

Ancak Yaz%Tıkla yöntemi PCCP ile kıyas edildiğinde anlamlı bir şekilde üstün olduğu görülmektedir. Sonuçların özet hali tablo 5-7'de sunulmuştur. Bu başarı

sonuçları ışığında 3. hipotezimizin doğruluğunu kısmen de olsa gösterir bir delilde elde etmiş oluruz. Yani Yaz&Tıkla yöntemiyle şifre belirleyen kullanıcılar, belirledikleri birden fazla şifre ile yaklaşık başarı oranında sisteme giriş yapabilmişlerdir.

Deney sırasında yapılan gözlemlerden şu sonuçlar çıkarılabilir. Kullanıcıların 2. deney esnasında 1. deneyden kazandıkları tecrübeyle yöntemlere yaklaşımı daha bilinçli oluşmuştur. Birçoğu Yaz&Tıkla yönteminin kazandırdığı avantajı daha iyi fark etmiş, şifrelerinde belirledikleri metin kısmının resimle doğrulamasını daha iyi kullanmışlardır. Kendileri için uygun resim gelenedek metin belirleme aşamasını kontrollü bir şekilde tamamlamışlardır. Sonrasındaki resim üzerinde nokta belirleme aşamasında görüntü kapısının tıklamayı düşündükleri noktaya gelmesi için çaba gösterdikleri görülmüştür. Zaten bu sonuç Yaz&Tıkla yönteminin "görüntü kapısının yerini değiştirme" değerinden de görülmektedir. Neredeyse bu değer PCCP yöntemindeki "yer değiştirme" değerler ortalamasının iki takını aşmıştır. Aynı zamanda bu sonuç resim sayısı arttıkça "yer değiştirme" değerinin azaldığını da gösteriyor olabilir.

Çizelge 5.6 İkinci Deney Başarı Oranları

	1. parola (90 gün sonra)			2. parola (45 gün sonra)		
	Başarılı	**Düzelterek Başardı**	**Başarısız**	**Başarılı**	**Düzelterek Başardı**	**Başarısız**
PCCP	21/39	3/39	18/39	22/39	15/39	17/39
	%53,85	%7,69	%46,15	%56,41	%38,46	%43,59
Yaz&Tıkla	28/39	3/39	11/39	30/39	2/39	9/39
	%71,79	%7,69	%28,21	%76,92	%5,13	%23,08
Metin	26/39	4/39	13/39	28/39	4/39	11/39
	%66,67	%10,26	%33,33	%71,79	%10,26	%28,21

Çizelge 5.7 İkinci Deney Başarı Durumu Özet Tablo

	1. parola (90 gün sonra)			2. parola (45 gün sonra)		
	Başarılı	**Başarısız**	**Başarı Oranı %**	**Başarılı**	**Başarısız**	**Başarı Oranı %**
PCCP	21	18	53,85	22	17	56,41
Yaz&Tıkla	28	11	71,79	30	9	76,92
Metin	26	13	66,67	28	11	71,79

Çizelge 5.8 Resim Üzerindeki "Görüntü Kapısı" nın yerini değiştirme sayısı (ikinci deney)

	PCCP			Yaz&Tıkla
	Resim 1	**Resim 2**	**Resim 3**	**Resim 1**
Ortalama	17,0	18,3	9,4	33,0
Ortanca	13	8	5	12

Yapılan bir diğer inceleme de, her ne kadar kullanıcıları farklı şifre belirlemeleri notasında uyarsak da yine aynı ya da benzer şifreyi belirleyen kullanıcılar olmuştur. Bu durum Yaz&tıkla yönteminde 6 kişi, Metin yönteminde ise 4 kişidir ve bu kullanıcılardan Metin yönteminde 4 kullanıcıda başarılı bir şekilde sisteme giriş yaparken, Yaz&Tıkla yönteminde 2 kişi şifrelerinin metin kısımları benzer olmasına rağmen ilk seferlerinde hatalı giriş yapmışlar daha sonra şifrelerini düzelterek sisteme giriş yapabilmişlerdir. Yaz&Tıkla yönteminde kullanıcı aynı metni şifrenin ilk kısmı olarak belirleyip aynı resme ulaşsa da, görüntü kapısını da önceki şifresinde belirlediği noktanın üzerinde getirmesi gerekmektedir, daha önce belirtildiği gibi görüntü kapısının konumu sistemin rastgele belirlediği farklı bir yerdir. Dolayısıyla sistem yine kullanıcıyı farklı bir şifre belirlemeye zorlamıştır. Bu durum PCCP yöntemi için tamamen farklıdır. Bu yöntemde resimler rastgele kullanıcıya gösterildiğinden şifreler doğal olarak farklı belirlenmek zorundadır.

5.2 Zaman Bilgileri

Tablo 5-9'da kullanıcıların şifre oluşturma, şifre doğrulama ve tekrar sisteme giriş yapma adımlarının her birisi için toplam harcadığı zaman bilgisi (saniye) sunulmuştur. Özetle, metin şifre yönteminde kullanıcıların daha hızlı oldukları, diğer iki yöntemde ise yaklaşık aynı seviyelerde zaman harcadıkları anlaşılmaktadır. Yaz&Tıkla yönteminde şifre oluşturma ve tekrar sisteme giriş yapma işlemlerinin fazla zaman almasının nedenini, deney esnasındaki gözlemlerimize dayanarak söyleyebiliriz ki, kullanıcılar şifrelerinin metin kısımlarını resimle doğrulama yaparak belirlemeleri fazla zaman almasına neden olmuştur. İstatistikî olarak zaman verilerini karşılaştırdığımızda Metin yönteminin anlamlı bir şekilde diğerlerinden ayrıldığını görmekteyiz.

Metin yöntemi, parola oluşturma aşamasında [$F(2\text{-}225)=29.529, p<0.000$] değeri ile, parola onaylama aşaması [$F(2\text{-}225)=18.797, p<0.000$] değeri ile ve ikinci defa sisteme giriş yapma aşaması [$F(2\text{-}225)=8.373, p<0.000$] değeriyle anlamlı sonuçlar vermiştir. Ancak yöntemler arasında, şifreyi belirledikten sonraki ilk defa parola girişi aşamasında ise [$F(2\text{-}225)=29.529, p<0.000$] değeri ile anlamlı bir fark olmadığı görülmüştür.

Çizelge 5.9 Zaman Bilgileri

		Parola Oluşturma	Parolayı Onaylama	Parolayı Girme	Parola Girme (45 gün sonra)
PCCP	**Ortalama**	43,8	17,5	20,7	43,9
	Ortanca	35,5	16,0	17,0	33,0
Yaz&tıkla	**Ortalama**	35,0	12,9	19,6	46,0
	Ortanca	26,5	11,0	18,5	30,0
Metin	**Ortalama**	16,0	9,9	17,0	26,1
	Ortanca	9,5	9,0	15,0	18,0

Çizelge 5.10 İkinci deneyin sonunda 2 parolanın sisteme giriş zamanları

		1.parola	2.parola
PCCP	**Ortalama**	24,00	29,45
	Ortanca	24,00	26,00
Yaz&tıkla	**Ortalama**	25,43	22,77
	Ortanca	19,00	19,50
Metin	**Ortalama**	16,35	17,64
	Ortanca	14,50	16,00

Şifrelerini sisteme hatasız bir şekilde girebilen kullanıcıların zaman değerleri tablo 5-11 ve tablo 5-12 ‘de gösterilmiştir. Hatasız parola girişi yapabilen kullanıcılar içinde Metin tabanlı yöntemin diğer yöntemlere nispeten daha kısa sürdüğü görülmektedir. Ayrıca Yaz&Tıkla yönteminin zaman değeri her iki şifre için PCCP yönteminden daha kısa sürdüğü görülmektedir. Dolayısıyla geliştirdiğimiz Yaz&Tıkla yöntemi, metin tabanlı yöntemden olmasa da PCCP yönteminden hatasız kullanımlarda daha hızlı sonuçlar verdiği görülmüştür.

Çizelge 5.11 Birinci Şifreler ile Sisteme Hatasız Giriş Yapabilen Kullanıcıların Zaman değerleri

		Parola Oluşturma	Parolayı Onaylama	Parolayı Girme	Parola Girme (45 gün sonra)
PCCP	**Ortalama**	43,42	13,52	17,54	32,29
	Ortanca	40,50	12,00	16,50	28,00
Yaz&Tıkla	**Ortalama**	33,72	10,82	18,82	31,53
	Ortanca	25,50	10,00	18,00	25,50
Metin	**Ortalama**	12,86	9,72	16,33	21,60
	Ortanca	9,00	9,00	14,00	18,00

Çizelge 5.12 İkinci Şifreler ile Sisteme Hatasız Giriş Yapabilen Kullanıcıların Zaman değerleri

		Parola Oluşturma	Parolayı Onaylama	Parolayı Girme	Parola Girme (45 gün sonra)
PCCP	**Ortalama**	35,54	10,92	15,77	26,55
	Ortanca	33,00	10,00	13,00	26,00
Yaz&Tıkla	**Ortalama**	36,50	10,79	14,82	22,77
	Ortanca	24,50	10,00	14,00	19,50
Metin	**Ortalama**	12,73	8,60	15,23	17,64
	Ortanca	10,00	8,00	14,00	16,00

5.3 Anket Sonuçları

Tablo 5-14 ve tablo 5-15' da, yapılan anket sonucunda elde edilen veriler sunulmuştur. Bu veriler kullanıcıların Yaz&Tıkla yöntemini daha güvenli ve daha kullanışlı bulduklarını göstermektedir. Sonuç olarak, anket yolu ile ikinci hipotezimiz için de bir delil elde ettiğimizi söyleyebiliriz.

Deney aşamasında kullanıcıları, Yaz&Tıkla ve Metin yöntemlerinden oluşturdukları şifrelerin "metin" kısımlarının farklı olması noktasında uyarsak da 18 kişi bu değeri aynı belirlemiştir. Ayrıca kullanıcıların anket sorularına verdiği cevapları, veri tabanımızdaki kullanıcı değerleri ile karşılaştırdığımızda 17 kişide şifrelerin "metin" kısımları farklı olsa da benzer değerler olarak belirlemişlerdir. Dolayısıyla toplamda 35 kişinin belirledikleri şifrelerinde "metin" kısımları aynı yada benzerdir. Bu kişileri çıkararak 42 kişinin Yaz&Tıkla ve Metin yöntemlerindeki başarı durumları tekrar değerlendirildiğinde Yaz&Tıkla yönteminin başarısının daha da arttığı görülmektedir. Başarı değerleri tablo 5-13'de gösterilmiştir.

Çizelge 5.13 Yaz&Tıkla ve Metin tabanlı yöntemlerin "metin" kısımları farklı olanların başarı değerleri

	Başarılı	Başarısız	Başarı Oranı %
Yaz&Tıkla	36	6	85,71
Metin	27	15	64,29

Çizelge 5.14 Anket Sonuçları

	Yaz&Tıkla	PCCP	Metin
1.soru: Hangi yöntemle şifre oluşturup kullanmayı tercih edersiniz?	51	15	10
2.soru: Şifrenizi en kolay hangi yöntemle oluşturabildiniz?	37	13	26
3.soru: Şifrenizi en kısa sürede hangi yöntemle oluşturabildiniz?	23	15	38
4.soru: Sizce hangi yöntem daha güvenlidir?	41	25	10
5.soru: Sizce hangi yöntemle oluşturulan şifreyi hatırlamak daha kolaydır?	43	11	22
6.soru: Bir banka hesabınızın şifresini belirlerken hangi yöntemi kullanırsınız?	39	25	12

Çizelge 5.15 Anket Sonuçları (devam)

	Evet	Hayır
7.soru: Yaz&Tıkla ve Metin yöntemindeki şifrelerin "metin" kısımları birbirinden farklı mı ?	58	18
8.soru: Kullandığınız şifreler daha öncekilerden farklı mı ?	74	2
9.soru: Yaz&Tıkla yöntemindeki resim, şifrenin "metin" li kısmını hatırlamanızı kolaylaştırdı mı ?	60	16

5.4 Hipotez Sonuçları

Geliştirdiğimiz yöntemle doğruluğunu ispat etmeye çalıştığımız hipotez sonuçlarını bu bölümde tekrar özetleyecek olursak;

1. Hipotez: "Yaz&Tıkla yöntemi ile belirlenen şifreler diğer iki yöntem ile belirlenen aynı güvenlik seviyesindeki şifrelere göre uzun vadede kullanıcılar tarafından daha iyi hatırlanacaktır."

Birinci deney sonunda elde edilen sonuçlar ışığında, geliştirdiğimiz Yaz&Tıkla hibrit yöntemin %80 başarı oranı, diğer yöntemlerin gösterdikleri başarı oranlarına göre istatistikî olarak daha anlamlı olduğu görülmüştür. Böylece 1. Hipotezin doğruluğu gösterilmiştir.

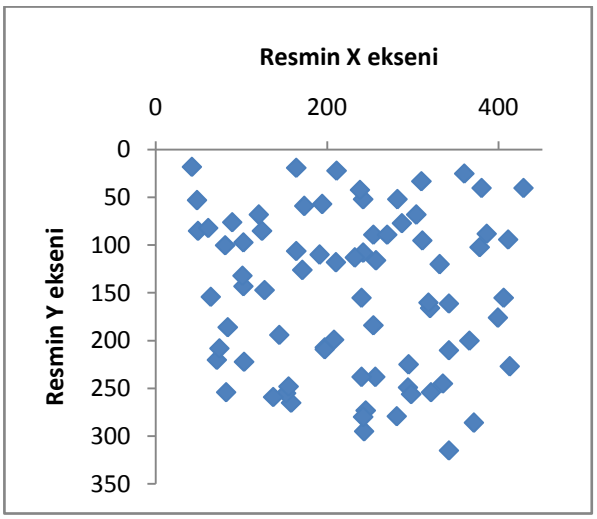
2. Hipotez: "Kullanıcılar Yaz&Tıkla yöntemi ile oluşturulan şifreleri diğerlerine nazaran daha güvenli ve daha kullanışlı olarak algılayacaktır."

Bir sistemin güvenli olması kadar kullanıcılar tarafından da güvenli bulunması o sistemin pratikte uygulanabilirliği açısından çok önemlidir. Deney sürecinde kullanıcılara uygulanan anketlerin sonuçları Yaz&Tıkla yönteminin diğer yöntemlere göre kullanıcılar tarafından daha güveni ve kullanışlı olarak tercih edilmiştir. Dolayısıyla 2. Hipotezinde doğruluğu gösterilmiştir.

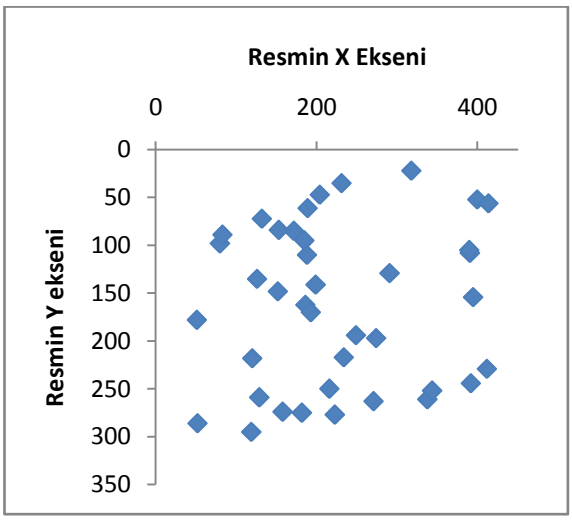
3. Hipotez: "Kullanıcı Yaz&Tıkla yöntemi ile oluşturduğu birden fazla şifreyi yaklaşık başarı oranı ile hatırlayacaktır."
Uygulanan ikinci deney sonucunda elde edilen veriler bu hipotezin kısmen ispatlandığını göstermektedir.
İkinci deney sonucunda Yaz&Tıkla yöntemi %76 başarı oranı ile metin tabanlı yönteme olmasa da PCCP grafik tabanlı yönteme göre anlamlı bir şekilde başarılı olduğu görülmüştür. Dolayısıyla 3. hipotezin doğruluğu kısmen gösterilmiştir.

5.5 Tıklanılan Nokta Değerleri

Bu bölümde kullanıcıları Yaz&Tıkla yöntemindeki resim üzerinde tıkladıkları noktaların analizi yapılmış ve noktaların rastgele dağılım gösterip göstermediği ve kümelenme oluşturup oluşturmadığı tespit edilmiştir. Bu çalışma sonuçlarına göre yöntemde kullanılan resimlerin "sıcak nokta" problemine karşı ne kadar güçlü olduğunu görebileceğiz. Kullanıcıların resim üzerinde tıkladıkların noktaların koordinatları şekil 5-1 ve şekil 5-2'de gösterilmiştir.
Rastgele dağılım olup olmadığını ve kümelenme olup olmadığını görebilmek için Spatstat analiz programı kullanılmıştır. [29] R programlama dilini kullanarak deney verilerini girebildiğimiz programda ihtiyacımız olan değer J istatistikî fonksiyonun ürettiği değerdir. [30] J fonksiyonu kullanıcıların tıkladığı noktaların koordinatlarını ve tolerans değerine göre (19x19 piksel) yaklaşık bir değer olarak r=9 sayısını parametre olarak alır ve 0 ile 1 arasında bir değer üretir. J değeri 1'e yakın olduğu nispette kümelenme olmadığını ve rastgele bir dağılım olduğunu gösterir. J(9)=1 değerini grafik şifreleme sistemleri için düşündüğümüzde, kullanıcını resim üzerinde tıkladığı noktayı saldırganın tahmin edebilmesi güç anlamına gelmektedir.

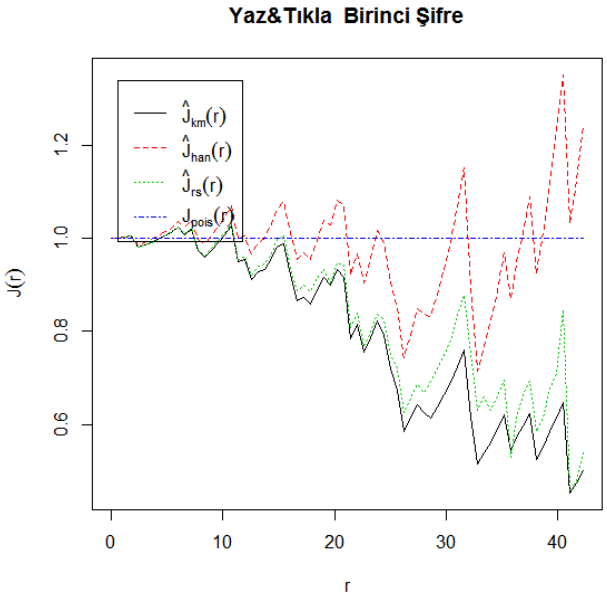


Şekil 5-1 Birinci deneyde kullanıcıların resim üzerinde tıkladıkları koordinatlar

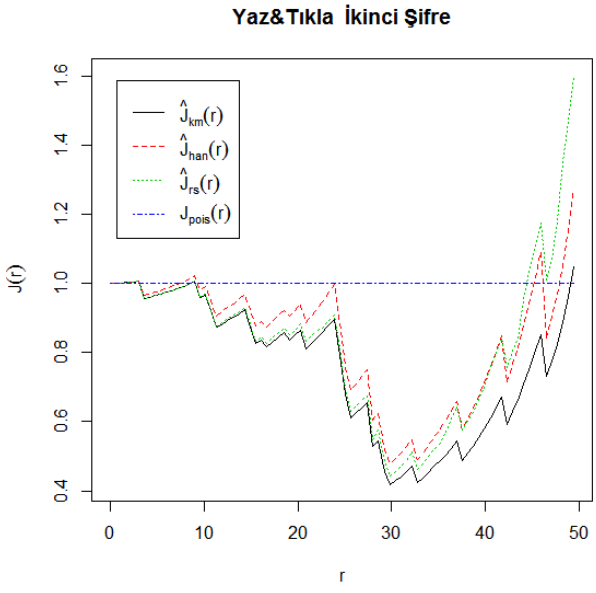


Şekil 5-2 İkinci deneyde kullanıcıların resim üzerinde tıkladıkları koordinatlar

Şekil 5-3 ve 5-4' de görüldüğü üzere J(9) değerlerini farklı yöntemlerle elde edilebilen tahmini sonuçlar (kırmızı,yeşil ve siyah renkle gösterilen çizgiler) için incelediğimizde hepsinin teorik olarak beklenilen değerde (mavi çizgi ile gösterilen) 1'e yaklaşık olduğu görülmüştür.



Şekil 5-3 Birinci Şifrede Tıklanılan Noktaların J Fonksiyon Değerleri



Şekil 5-4 İkinci Şifrede Tıklanılan Noktaların J Fonksiyon Değerleri

BÖLÜM 6 - SONUÇ

Kimlik doğrulama sistemleri her ne kadar farklı yöntemlerle farklı platformlarda sağlanacak olsa da güncelliğini sürekli koruyacak ve önemi her geçen gün artacak bir konudur. Çünkü her yeni sistem kullanıcılarına uzaktan erişim ve kullanım kolaylığı sağlamak üzere geliştirilmektedir. Uzaktan erişim, yetkilendirme ve kullanım hizmetleri kimlik doğrulama yöntemlerine ihtiyacı doğurmuştur. Günümüzde en yaygın kullanılan doğrulama yöntemi ise metin tabanlı kimlik doğrulama yöntemidir. Yıllardır kullanımı devam eden metin tabanlı yöntemin zamanla bazı zayıf yönleri iyice kendini hissettirmektedir. Bu zayıf yönlerini kullanan kötü niyetli saldırganlar, birçok farklı yöntemlerle şifreleri ele geçirebilmektedirler. Şifrelerini saldırganlara kaptıran kullanıcılar bazen hesap edilemeyecek kadar maddi ve manevi zarara maruz kalabilirler. Metin tabanlı yöntemin zayıf yönleri farklı, alternatif çözümlere ihtiyacı doğurmuştur. İnsan hafızasını metinlerden çok resim ya da görsel öğeleri daha kolay hatırlayabildiği gerçeğinden yola çıkarak geliştirilen grafik tabanlı kimlik doğrulama yöntemleri şimdilik iyi bir alternatif olarak görülmektedir. Zamanla geliştirilen, farklı yöntemlere sahip grafik şifreleme yöntemleri avantaj ve dezavantajlarıyla önceki bölümlerde sunulmuştur.

Kullanıcıların uzun yıllardır metin tabanlı parolaları kullanmaları ve genel bir alışkanlık elde edinmeleri sebebiyle grafiksel şifre yöntemlere ani ve hızlı bir geçişin mümkün olmadığını düşünüyoruz. Bu düşünceden hareketle bu çalışmada metin ve grafiksel öğeleri birleştiren Yaz&Tıkla yöntemini önermekteyiz. Tarafımızca yönetilen ve sonuçlarını yukarıda incelediğimiz laboratuar deneyi ile Yaz&Tıkla yönteminin kullanışlılık avantajlarının olabileceğine dair ipuçları elde edilmiştir.

BÖLÜM 7 - KAYNAKLAR

[1]. *Kullanışlı Güvenlik için Temel Prensipler.* **Bıçakcı, Kemal.** ANKARA, TÜRKİYE : 4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 6-8 Mayıs 2010.

[2]. **Yüceel, Mustafa.** Güvenli ve Kullanışlı Resim-Şifre Yöntemlerinin Tasarlanması ve Gerçekleştirilmesi. *Yüksek Lisans Tezi.* ANKARA : TOBB Ekonomi ve Teknoloji Üniversitesi, 2010.

[3]. *A Usability Study and Critique of Two Password Managers.* **Chiasson, S., van Oorschot, P.C., Biddle, R.** August, 2006. s. In Proceedings of 15th USENIX Security Symposium.

[4]. *Graphical Passwords as Browser Extension: Implementation and Usability Study.* **Bıçakcı, Kemal, et al.** Purdue University,West Lafayette, USA : In Proc. Third IFIP WG 11.11 International Conference on Trust Management, June 15-19, 2009.

[5]. **Burr, William E., Dodson, Donna F. ve Polk, W. Timothy.** *Electronic Authentication Guideline.* Gaithersburg,MD USA : National Institute of Standards and Technology (NIST), April,2006.

[6]. *A survey of password mechanisms: Weaknesses and potential improvements.* **Jobusch, David L. ve Oldehoeft, Arthur E.** s.l. : Iowa State University, Computer Science Department, Ames, IA, U.S.A, 11 April 2002.

[7]. **Yan, J., et al.** *Password memorability and security: empirical results.* s.l. : IEEE Security and Privacy magazine 2(5), 25-31, 2004.

[8]. **Gutmann, Peter.** Security usability. [Çevrimiçi] February 2008. http://www.cs.auckland.ac.nz/~pgut001/pubs/usability.pdf.

[9]. *Human selection of mnemonic phrase-based passwords.* **Kuo, C., Romanosky, S. ve Cranor, L.F.** s.l. : SOUPS 2006.

[10]. *Graphical Passwords:Learning from the First Generation.* **Biddle, Robert, Chiasson, Sonia ve Oorschot, P.C. van.** Carleton University, Ottawa, Canada : School of Computer Science, October 2, 2009.

[11]. *Graphical Passwords: Learning from the First Twelve Years.* **Biddle, Robert, Chiasson, Sonia ve Oorschot, P.C van.** Carleton University : School of Computer Science, january 4,2011.

[12]. **Kirkpatrick, B.** Psychological Review. *An experimental study of memory.* 1894.

[13]. *Why are pictures easier to recall than words?* **Paivio, A., Rogers, T. ve Smythe, P.** s.l. : Psychonomic Science, 11(4), 1968.

[14]. *Influencing Users Towards Better Passwords: Persuasive Cued Click-Points.* **Chiasson, Sonia, et al.** Liverpool UK : Published by the British Computer Society, 2008. Human-Computer Interaction Conference (HCI 2008).

[15]. *Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords.* **Chiasson, Sonia, et al.** Chicago,Illinois, USA : s.n., November 9–13, 2009.

[16]. *A Research Agenda Acknowledging the Persistence of Passwords.* **Herley, Cormac ve Oorschot, Paul C. van.** s.l. : IEEE Security&Privacy Magazine in early 2012, August 25, 2011.

[17]. *Influencing Users Towards Better Passwords: Persuasive Cued Click-Points.* **S.Chiasson, et al.** s.l. : HCI 2008, September 1-5 2008.

[18]. **Blonder, G.** *United states patent. 5559961* 1996.

[19]. *A Multi-Word Password Proposal (gridWord) and Exploring Questions about Science in Security Research and Usable Security Evaluation.* **Bıçakcı, Kemal ve Oorschot, P.C. van.** Marin County, CA, US : New Security Paradigms Workshop (NSPW 2011), Sept.12-15.

[20]. *Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism.* **Chiasson, Sonia, et al.** Oct 2011, IEEE Transaction on Dependableand Secure Computing (TDSC).

[21]. *Are Passfaces More Usable Than Passwords? A Field Trial Investigation.* **Brostoff, Sacha ve Sasse, M. Angela.** s.l. : Department of Computer Science, University College London,London, WC1E 6BT.

[22]. *Support for Authoring and Managing Web-Based Coursework: The TACO Project.* **M.A, Sasse, C, Harris ve I, Ismail.** Cilt The Digital University: Reinventing the Academy, Springer-Verlag, pp.155-175.

[23]. *Deja Vu: A User Study Using Images for Authentication.* **Dhamija, Rachna ve Perrig, Adrian.** s.l. : SIMS / CS, University of California Berkeley.

[24]. *TwoStep: An Authentication Method Combining Text and Graphical Passwords.* **van Oorschot, P.C. ve Wan, Tao.** School of Computer Science, Carleton University, Ottawa, Canada : s.n.

[25]. *A Hybrid Graphical Password Based System.* **Khan, Wazir Zada, et al.** s.l. : Springer-Verlag Berlin Heidelberg, 2011.

[26]. *Evaluation of a Usable Hybrid Authentication System.* **Olanrewaju, Ayannuga O, Olusegun, Folorunso ve Akinwale, Adio.** s.l. : International Journal of Computer Applications, Volume 17– No.8, March 2011.

[27]. **NIST.** *National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy.* June 25, 2010.

[28]. *Persuasive technology: using computers to change what we think and do.* **Fogg, B. J.** s.l. : Morgan Kaufman Publishers , San Francisco, CA,2003.

[29]. *spatstat: An R Package for Analyzing Spatial Point Patterns.* **Baddeley, Adrian ve Turner, Rolf.** s.l. : Journal of Statistical Software, 2005.

[30]. *A nonparametric measure of spatial interaction in point patterns.* **Lieshout, M.van ve Baddeley, A.** s.l. : Statistica Neerlandica, 1996.

[31]. *A Hybrid Graphical Password Based System*. **Khan, Wazir Zada,** et al. s.l. : Springer-Verlag Berlin Heidelberg, 2011.

[32]. *Evaluation of a Usable Hybrid Authentication System*. **Olanrewaju, Ayannuga O, Olusegun, Folorunso ve Akinwale, Adio**. s.l. : International Journal of Computer Applications, Volume 17– No.8, March 2011.

Ek A- Web Tabanlı Şifre Doğrulama Yöntemi

Bu tez çalışması ile geliştirdiğimiz Yaz&Tıkla yöntemini son haline getirmeden önce yöntemin gelişiminin ilk evresi bu bölümde anlatılacaktır.

İlk etapta web tabanlı olarak tasarladığımız yöntemde, kullanıcıya sisteme giriş esnasında, şifresini hemen yanında, şifresinin her bir karakterini girdikçe dinamik olarak beliren resim sayesinde, şifresini doğrulayarak sisteme girmesini sağlayacak bir yöntem geliştirdik. (Şekil Ek A.1)

Şekil Ek A.1 Web Tabanlı Şifre Doğrulama

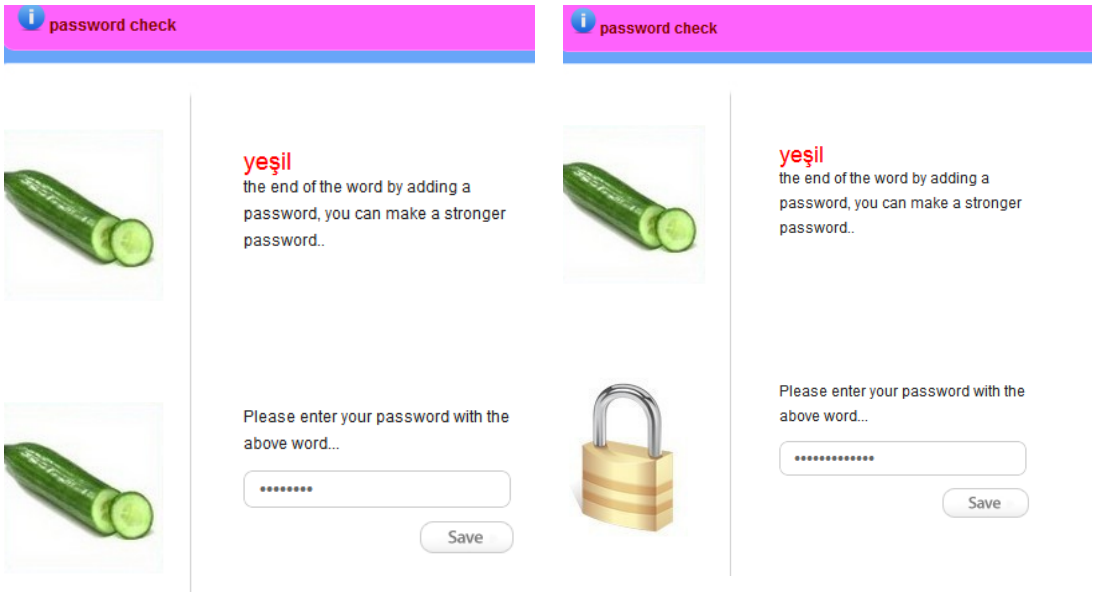
Kullanıcı şifresinin karakterlerini girdikçe resmin dinamik olarak değişmesi fikri metin ve grafik öğeleri birleştirmek adına özgün bir yöntemdir.

Yöntemin çalışması ise şu şekildedir;

Kullanıcı sisteme kaydolup metin tabanlı şifresini belirlediği esnada girdiği her bir karakterle resimlerinde değiştiğini görür ve şifresini tamamladığında, sistemin belirlenen şifreye göre atadığı resim kullanıcıya son olarak gösterilir. Kullanıcı bu resim sayesinde her ne zaman sisteme giriş yapacak olsa, şifresini yazıp aynı resme ulaşabildiği takdirde şifresini doğru yazdığına emin olur.

Ek B- Web Tabanlı Şifre Güçlendirme Yöntemi

Ek A'da anlatılan şifre doğrulama yöntemi üzerine bazı eklentiler yaparak şifrenin güçlendirilmesi amaçlanmıştır.



Şekil Ek B.2 Web Tabanlı Şifre Güçlendirme

Şifre güçlendirmek amacıyla yöntemde yaptığımız değişiklik de;
Kullanıcı şifresini belirlerken yine dinamik olarak küçük resimlerin değiştiğini görür. - bu aşamaya kadar Ek 1'de anlatılan bölümdür- Kullanıcı şifresinin son halini belirlediğinde sistemde şifresine karşılık bir resmi kullanıcıya gösterir. Kullanıcı bu resim sayesinde şifresini doğrulayabileceğini bilir. Bu aşamadan sonra kullanıcıya, şifresini güçlendirmek istediği takdirde sistem, belirlenen şifreye karşılık gelecek şekilde resmi tanımlayan bir de kelime gösterilir. Kullanıcıdan şifresinin sonuna resimle ilişkilendirilmiş bu kelimeyi de eklemesi istenir. Dolayısıyla karakter sayısı artan şifre, öncekine nispeten daha güçlü bir hal alır.
Şekil Ek-2'de gösterildiği gibi kullanıcının şifresine karşılık sistemin atadığı resim "salata" olmuş ve resimle ilişkilendirilmiş "yeşil" kelimesini şifresinin sonuna eklemesi istenmiştir. Kullanıcı bu kelimeyi de eklediğinde, sistemin kullanıcıya atadığı yeni resim "kilit" olmuştur. Bu şekilde kullanıcı hem şifresini güçlendirmiş

hemde dinamik olarak değişen resimler sayesinde sisteme giriş yapmadan şifresini doğrulama imkânı bulmuştur.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : AKPULAT, Murat

Uyruğu : T.C.

Doğum tarihi ve yeri : 12.06.1984 Bayburt

Medeni hali : Evli

Telefon : 0 (505) 399 73 72

e-mail : makpulat@etu.edu.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Yüksek Lisans	TOBB Ekonomi ve Teknoloji Üniversitesi (Bilgisayar Mühendisliği)	2012
Lisans	Ondokuz Mayıs Üniversitesi (Bilgisayar ve Öğretim Teknolojileri)	2008

İş Deneyimi

Yıl	Yer	Görev
2009- (halen)	Gümüşhane Üniversitesi (Bilgisayar Teknolojileri Bölümü)	Okutman Bölüm Başkanı

Yabancı Dil

İngilizce

Yayınlar

M Akpulat, K Bıçakcı, U Çil**,** Metin ve Grafiksel Öğeleri Birleştiren Yeni Bir Parola Tabanlı Kimlik Doğrulama Yöntemi, 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, iscTurkey2012, sayfa 75-80, ANKARA/TÜRKİYE