Metin ve Grafiksel Öğeleri Birleştiren Yeni bir Parola Tabanlı Kimlik Doğrulama Yöntemi

Murat AKPULAT, Kemal BIÇAKCI, Uğur ÇİL

Özet— **Günümüzde en yaygın kullanılan kimlik doğrulama yöntemi şifre (parola) tabanlı olanlardır. Son yıllarda pek çok grafiksel parola yöntemleri geliştirilmiş fakat bu yöntemler pratikte henüz klasik metin parolaların yerini alamamıştır. Bu çalışmada hem metin hem grafiksel öğeler içeren melez bir parola tabanlı kimlik doğrulama yöntemi önermekteyiz. Yaptığımız deneysel çalışma Yaz&Tıkla ismini verdiğimiz yeni yöntemin hem uzun dönem hatırlanabilirlik hem de kullanıcı memnuniyeti açısından sadece metin ve sadece grafik tabanlı parola yöntemlerine oranla daha başarılı olduğunu göstermektedir.**

Anahtar Kelimeler—**Kullanışlı Güvenlik, Grafik Şifre, Resim Şifre, Parola, Kimlik Doğrulama.**

Abstact— **Today, the most widely used authentication methods are password based. In recent years, many graphical password methods have been developed but these methods could not replace traditional text passwords, yet. In this work, we propose a hybrid method called Type&Click which incorporates both text and graphical elements. We conduct a usability study which shows that with respect to long-term memorability and user satisfaction, Type&Click is more successful as compared to only-text and only-graphical password methods.**

Keywords—**Usable Security, Graphical Password, Password, Authentication**

I. GİRİŞ

METİN tabanlı klasik parola (şifre) en iyi bilinen ve en yaygın kullanılan kimlik doğrulama yöntemidir. 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 [1] 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,*

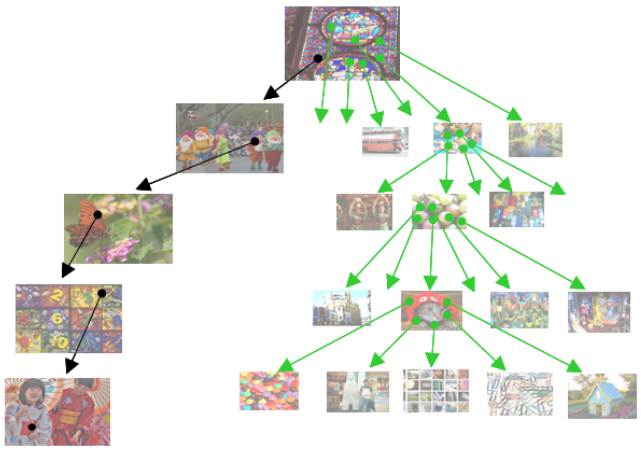
bu yazılım (donanım, sistem) Kullanışlı Güvenlik (usable security) özelliğine sahiptir."

İnsan beyninin resimleri hatırlayabilmesinin metinlere oranla daha kolay olduğunu ortaya koyan çalışmalar [2] sonrasında başlatılmış ve metin tabanlı yöntemlere alternatif sunmayı hedefleyen grafiksel yöntemler konusunu 'kullanışlı güvenlik' bağlamında incelemek gerekir. Daha açık ifadeyle, yeni yöntemlerin tercih edilmesi için metin tabanlı parola yöntemine göre belirgin kullanışlılık ve/veya güvenlik avantajlarına sahip olmaları şarttır. Fakat önceki çalışmaları incelediğimizde neredeyse tamamının yapmış oldukları deneysel değerlendirmelerde (hatırlanabilirlik, giriş süresi, vb. metrikleri kullanarak) önceki benzer grafiksel yöntemler ile karşılaştırmalarda bulunmuş oldukları görülmektedir [3]. Bu hususta bir istisna araştırmacıların PCCP sistemini [4] değerlendirirken Passpoints sisteminin yanı sıra metin tabanlı şifreler ile de yapmış oldukları karşılaştırmadır. Bizim bu çalışmamızı önceki pek çok çalışmadan ayıran birinci fark deneysel karşılaştırma için klasik metin tabanlı şifrelerin seçilmesi ve böylece daha gerçekçi ve yönlendirici sonuçların ortaya konulmasına çalışılmış olunmasıdır.

M. Akpulat, Gümüşhane Üniv., Kelkit Aydın Doğan M.Y.O., Bilgisayar Teknolojileri Bölümü, Okutman ve TOBB Ekonomi ve Teknoloji Üniversitesi, Bilgisayar Mühendisliği Bölümü, Yüksek Lisans Öğrencisi. (telefon: 90-456-3173992, faks: 90-456-3173993, e-posta: muratakpulat@gumushane.edu.tr).

K. Bıçakcı, TOBB Ekonomi ve Teknoloji Üniversitesi, Bilgisayar Mühendisliği Bölümü, Doç. Dr. (telefon: 90-312-2924262, faks: 90-312-2924180, e-posta: bicakci@etu.edu.tr).

U. Çil, TOBB Ekonomi ve Teknoloji Üniversitesi, Bilgisayar Mühendisliği Bölümü, Yüksek Lisans Öğrencisi, e-posta: ucil@etu.edu.tr.



Şekil 1. CCP ve PCCP yöntemlerinin çalışma prensibi [3] (tıklanılan noktaya bağlı olarak bir sonraki resim belirlenir).

Çalışmamızın konu literatürüne ikinci ve daha önemli bir katkısı metin ve grafiksel öğeleri birleştiren bir şifre yönteminin ilk defa deneysel olarak incelenmesi ve hem metin tabanlı hem de grafik tabanlı şifre yöntemleri ile karşılaştırılmasıdır (benzer bir melez yöntem daha önce önerilmiş, fakat deneysel olarak incelenmemiştir [5]). Bu makalede, tarafımızca geliştirilen Yaz&Tıkla (Type&Click) ismini verdiğimiz melez kimlik doğrulama yönteminin tasarım aşamaları, deney süreci ve değerlendirme sonuçları sunulmaktadır. Deney sonuçları ışığında Yaz&Tıkla yönteminin mevcut metin tabanlı parola yöntemlerine kullanışlı bir alternatif sunduğunu söyleyebiliriz.

Çalışmamızın ikinci bölümünde literatür özetine yer verilmiş ve grafik şifre sistemlerinin bazı özelliklerinden bahsedilmiştir. Bölüm 3'de karşılaştırılacak yöntemlerin teknik incelemesi yapılmıştır. Bölüm 4'de geliştirdiğimiz yöntemi karşılaştırabilmek için kullanılan deneysel metodoloji tanıtılmıştır. Bölüm 5'de deney sonrası elde edilen veriler sunulmuş ve yorumlanmıştır. Son olarak bölüm 6'da yapılan çalışmadan elde edilen sonuçlar özetlenmiştir.

II. LİTERATÜR ÖZETİ

Bilgi-tabanlı (veya parola-tabanlı) kimlik doğrulama (knowledge-based authentication) şu mantığa dayanır: Kişilerle sistem arasında gizli bir bilgi sır olarak paylaşılmaktadır ve sistem bu bilgiyi doğru olarak sağlayabilen kişinin, o kişinin kendisi olduğunu kabul ederek gerekli yetkilendirmeyi yapmaktadır. Burada bahsedilen gizli bilgi farklı şekillerde karşımıza çıkabilir. Örneğin kullanıcının ezberlediği ve biliyor olması gereken bir bilgi veya kullanıcının ezberlemesi gerekmeyen ancak gördüğünde tanıması gereken bir bilgi gibi.

Bilgi-tabanlı kimlik tanımlama yöntemleri iki başlık altında incelenebilir.

A. Metin Tabanlı Şifre Yöntemleri

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.

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 [6].

B. Grafik Tabanlı Şifre Yöntemleri

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 [2]. Grafik tabanlı sistemler kullanıcının daha kolay hatırlayabileceği görsel öğeleri kullanarak farklı bir yaklaşım getirmişlerdir.

Bazı grafik şifreleme sistemlerinde kullanıcının bir resim kümesi içinden seçtiği bazı resimleri sistem girişi sırasında tekrar tanıması beklenir. PassFaces yöntemi kullanıcıdan yüz resimlerinin olduğu bir kümeden 4 tanesini seçmesini ister. Kullanıcının şifresi bu 4 yüz resmidir ve 4 aşamada şifresini sisteme girer. Her bir aşamada 8 çeldirici resim ve 1 de kullanıcının seçtiği yüz resimlerinden bir tanesi bulunur [3].

Grafik kimlik doğrulama sistemlerinin bazılarında ise bir büyük resmin belli bir bölgesinde yapılan tıklamanın belli bir tolerans aralığında yeniden yapılması beklenir. Grafik şifreleme yöntemlerinden PassPoints bu mantıkla çalışır [3]. Sistem kullanıcıya bir resim gösterir ve kullanıcı resimde 5 farklı noktaya tıklayarak şifresini oluşturur. Kullanıcı ne zaman sisteme giriş yapacak olsa belli tolerans aralıkları dahilinde aynı resimde aynı noktalara tıklayarak sisteme giriş yapabilir.

Passpoints sistemini daha da geliştiren Cued Click Points (CCP) yönteminde ise kullanıcıya bir resim gösterilir ve bir noktayı tıklaması istenir [3]. Sistem kullanıcının tıkladığı noktaya göre farklı bir resim gösterir ve kullanıcı şifresinin ikinci elemanını bu farklı resimdeki bir noktaya tıklayarak girer. Bu şekilde tıklanılan noktaya göre gelen farklı resimlerde toplam 5 tıklama işlemiyle kullanıcı şifresini belirlemiş olur. Her bir resim bir önceki resimde tıklanılan noktaya göre seçildiği için kullanıcı resimlere tıklarken karşılaştığı resimlerden çıkarım yaparak şifresini doğru girip girmediğini kontrol edebilir. Gösterilen her bir resim kullanıcıya ipucu olur.

PCCP yöntemi, CCP ve Passpoints sistemlerinde gözlemlenen sıcak nokta problemini çözme adına önerilmiştir [4]. Sıcak noktalar, kullanıcının resim üzerinde tıklama ihtimalinin yüksek olduğu noktalardır. Tıklanması tahmin edilebilir bir nokta güvenlik açığı olarak düşünülebilir. PCCP, İkna Teknolojisinden (Persuasive Technology) yararlanmıştır. Kullanıcı bu yöntemde resim üzerinde istediği noktaya değil de sistemin kendisine sunduğu resim üzerindeki görüntü kapısı (viewport) içinden herhangi bir noktaya tıklayabilir. Ancak kullanıcı isterse görüntü kapısının tekrar oluşturulmasını isteyebilir ama yeni görüntü kapısı yine resim üzerindeki rastgele bir konumdadır. Bu sistem kullanıcıyı daha güçlü şifre belirlemeye teşvik eder (Şekil 2'de gösterilen Yaz&Tıkla yönteminde de görüntü kapısı kullanılmaktadır).

Bu makalede karşılaştırılacak PCCP ve Yaz&Tıkla yöntemlerinde görüntü kapısı kullanılacaktır. Resim 451x331 piksel çözünürlükte ve görüntü kapısı 75x75 piksel büyüklüğündedir (Şekil 2). Diğer teknik özellikler üçüncü bölümde anlatılacaktır.

C. Şifre Uzayı 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 [7]. Benzer durum sıcak nokta probleminden ötürü grafik tabanlı şifrelerde de söz konusu olabilir [3]. Fakat PCCP yönteminde sıcak nokta probleminin ihmal edilebilir seviyelerde kaldığı gözlemlenmiştir [4].

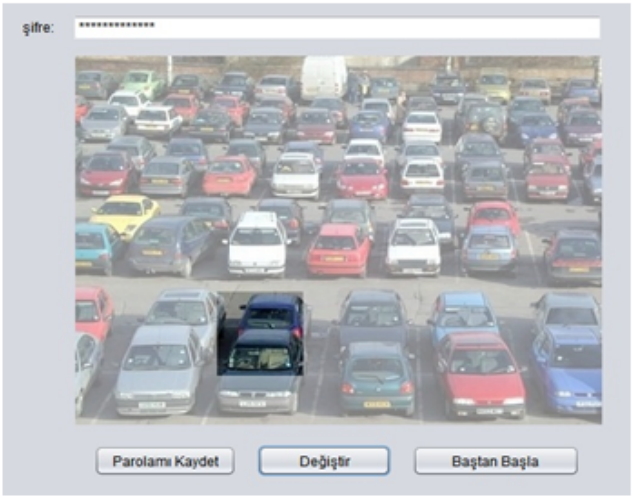
Belirsizliğin bir ölçütü olarak tanımlanan entropi, bilgi kuramında bilginin belirsizliği anlamına gelir. Şifreler bağlamında ise, belirlenen şifrenin belirsizliği ve dolayısıyla şifrenin gücünü nicel olarak ifade eden bir ölçüttür [7]. Entropi değeri yukarıdaki örnekte yaklaşık $\log_2(94^8) = 52{,}4$ bittir.

III. KARŞILAŞTIRALACAK 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,

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



Şekil 2. Yaz&Tıkla yöntemi şifre-giriş kullanıcı arayüzü (kullanıcı, metin şifresi ile ve görüntü kapısı içerisinde yapmış olduğu bir tıklama ile parolasını oluşturur).

Bu üç aşamayı da başarıyla gerçekleştiren kullanıcı ilgili yöntem ile kendine ait bir hesap oluşturmuş olur.

Aşağıda her alt bölümde yöntemlerin teknik özellikleri açıklanacaktır. Tüm yöntemler Java programlama dilinde masaüstü programlar olarak yazılmıştır.

A. Metin Tabanlı Şifre Yöntemi

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 [7] (diğer iki yöntemde de belirlenen şifreler aynı entropi değerine sahiptir).

B. PCCP

PCCP'de kullanıcı art arda gelen resimler üzerinde birer kez tıklayarak şifresini oluşturur (Şekil 1). 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. 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.

Şifre doğrulaması için kullanıcıdan bir önceki adımda oluşturduğu şifresini tekrar girmeleri istenecektir. 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.

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

$$[\frac{451x331}{19^2}]^3 \cong 2^{27} \quad (1)$$

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

C. Yaz&Tıkla Şifre Yöntemi

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. Bu sayfada kullanıcının şifresinin ilk kısmını oluşturabilmesi için bir metin giriş alanı ve girilen şifreye bağlı olarak dinamik olarak değişen bir resim vardır.

Kullanıcı metin giriş kısmına en az 8 karakterlik bir şifre girer. Belirlenen bu şifreye göre sistem kullanıcıya bir resim (451x331) gösterir ve resimde görüntü kapısı sınırları (75x75) içinde olmak koşulu ile bir tek noktaya tıklanması istenir (Şekil 2). 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.

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.

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 [7]. 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.

IV. 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).

Aşağıda, belirlenen hipotezleri test etmek için tasarlanan deneyde takip edilecek metodoloji kısaca tanıtılmaktadır.

Deneysel laboratuar çalışmamız Kelkit Aydın Doğan Meslek Yüksekokulu Bilgisayar Teknolojileri bölümü öğrencilerinden 39 kişinin katılımı ile gerçekleştirilmiştir. Kullanıcıların tamamı e-posta, alış-veriş, vb. şifre gerektiren siteleri aktif olarak kullanabilmektedirler.

Deney 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.

Tablo 1
Test edilen üç yöntem için birinci ve ikinci aşamadaki başarı oranları

	Parolayı Girme (ilk gün)		Parolayı Girme (45 gün sonra)		
	Başarılı	Düzelterek Başarılı	Başarılı	Düzelterek Başarılı	Başarısız
PCCP	36/39	3/39	7/39	17/39	15/39
	92,31%	7,69%	17,95%	43,59%	38,46%
Yaz&Tıkla	36/39	3/39	25/39	6/39	8/39
	92,31%	7,69%	64,10%	15,38%	20,51%
Metin	35/39	4/39	16/39	5/39	18/39
	89,74%	10,26%	41,03%	12,82%	46,15%

Tablo 2
Test edilen üç yöntem için ikinci aşama başarı sonuçlarının özeti

Parola Girme (45 gün sonra)	Başarılı	Başarısız	Başarı Oranı %
PCCP	24	15	61,54
Yaz&Tıkla	31	8	79,49
Metin	21	18	53,85

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 farklı kullanıcı grupları için farklı seçilmiştir. 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. Anket çalışması ile ikinci aşama sonlanmıştır.

V. SONUÇLAR VE DEĞERLENDİRME

Toplanan veriler ışığında ulaşılan sonuçlar aşağıda özetlenmiştir.

A. Başarı Oranları

Bu bölümde 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 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 2'de Düzelterek Başarılı ve Başarılı sonuçları "Başarılı" başlığı altında birleştirilerek ikinci aşamada elde edilen sonuçlar tekrar özet bir şekilde sunulmuştur. Tablo 2'de görüleceği üzere Yaz&Tıkla yöntemi yaklaşık % 80 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. [$p<0.052$]. 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.

Tablo 3
PCCP ve Yaz&Tıkla yöntemlerinde "değiştir" düğmesinin kullanılma sayıları

	PCCP			Yaz&Tıkla
	Resim1	Resim2	Resim3	Resim1
Ortalama	14,2	9,5	8,7	11,3
Ortanca	5	7	4	7

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 durum PCCP'de

Tablo 4
Test edilen üç yöntemde kullanıcıların her bir adımda harcadıkları zaman bilgileri

Toplam süre (ortalama)	Parola Oluşturma	Parolayı Onaylama	Parolayı Girme	Parola Girme (45 gün sonra)
Yaz&Tıkla	35,9	14,1	21,4	35,5
Metin	20,3	9,6	16,0	22,4
PCCP	44,6	17,6	21,6	35,6

de vardır. Ancak kullanıcıların resimler üzerinde tıklama işlemlerini birkaç defa denemesi ve beğenmediği resmi değiştirmek için önceki resme dönüp tekrar nokta belirlemesi esnasında kimi zaman konsantrasyon kaybına ve hatalara sebep olduğu gözlemlenmiştir. Kullanıcıların görüntü kapısını toleranslı 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 3'de PCCP ve Yaz&Tıkla yönteminde değiştir düğmesini kullanma 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.

B. *Zaman Bilgileri*

Tablo 4'de 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.

C. *Anket Sonuçları*

Tablo 5'de 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.

Tablo 5
Yapılan anket sonucunda elde edilen sonuçlar

Anket Soruları	Yaz&Tıkla	PCCP	Metin
1.soru: Hangi yöntemle şifre oluşturup kullanmayı tercih edersiniz?	26	8	5
2.soru: Şifrenizi en kolay hangi yöntemle oluşturabildiniz?	19	7	13
3.soru: Şifrenizi en kısa sürede hangi yöntemle oluşturabildiniz?	12	8	19
4.soru: Sizce hangi yöntem daha güvenlidir?	21	13	5
5.soru: Sizce hangi yöntemle oluşturulan şifreyi hatırlamak daha kolaydır?	22	6	11
6.soru: Bir banka hesabınızın şifresini belirlerken hangi yöntemi kullanırsınız?	20	13	6

VI. SONUÇ

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 özetle incelediğimiz laboratuar deneyi ile Yaz&Tıkla yönteminin kullanışlılık avantajlarının olabileceğine dair ipuçları elde edilmiştir. Fakat yapılan pilot çalışma ile yetinmemek gerekir. Daha geniş kapsamlı deneyler, saha çalışmaları, farklı katılımcı profilleri ile yapılan denemeler gibi ilave çalışmaların yürütülmesi tarafımızca planlanan çalışmalar arasındadır.

KAYNAKLAR

[1] Bıçakcı, K. (6-8 Mayıs 2010). Kullanışlı Güvenlik için Temel Prensipler. 4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.
[2] Paivio, A., Rogers, T., Smythe, P. (1968). Why are pictures easier to recall than words? Psychonomic Science, 11, 1-2.
[3] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comp. Surv., vol. 44,2012.
[4] Chiasson, S., Stobert, E., Forget, A., Biddle, R., P.C. van Oorschot (Oct 2011). Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Transaction on Dependable and Secure Computing (TDSC)* .
[5] P.C. van Oorschot, T. Wan. TwoStep: An Authentication Method Combining Text and Graphical Passwords. MCETECH 2009: 4th International MCETECH Conference on eTechnologies, 4-6 May 2009.
[6] Kuo, C., Romanosky, S., Cranor, L. Human selection of mnemonic phrase-based passwords. SOUPS 2006.
[7] Burr, W. E., Dodson, D. F., Polk, W. T. (April,2006). *Electronic Authentication Guideline.* Gaithersburg,MD USA: National Institute of Standards and Technology (NIST).