ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

HİBRİT RESİMLERİ KULLANAN OMUZ SÖRFÜNE KARŞI DİRENÇLİ GRAFİK TABANLI KİMLİK DOĞRULAMA

Başak BİLGİ

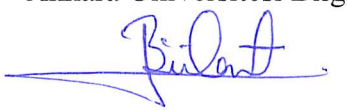
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI

ANKARA
2018

TEZ ONAYI

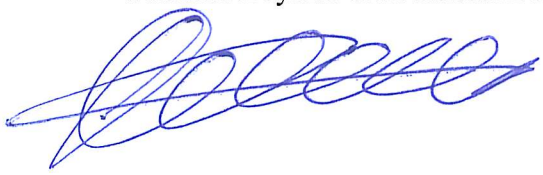
Başak BİLGİ tarafından hazırlanan "**Hibrit Resimleri Kullanan Omuz Sörfüne Karşı Dirençli Grafik Tabanlı Kimlik Doğrulama**" adlı tez çalışması 06/06/2018 tarihinde aşağıdaki jüri tarafından oy birliği ile Ankara Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Dr. Öğr. Üyesi Bülent TUĞRUL
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

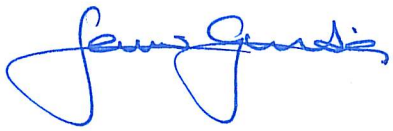


Jüri Üyeleri:

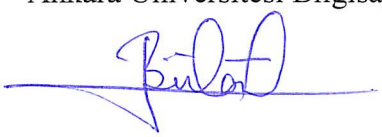
Başkan: Prof. Dr. Fatih V. ÇELEBİ
Yıldırım Beyazıt Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı



Üye : Doç. Dr. Semra GÜNDÜÇ
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı



Üye : Dr. Öğr. Üyesi Bülent TUĞRUL
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı



Yukarıdaki sonucu onaylarım.

Prof. Dr. Atila YETİŞEMİYEN
Enstitü Müdürü

ETİK

Ankara Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez içindeki bütün bilgilerin doğru ve tam olduğunu, bilgilerin üretilmesi aşamasında bilimsel etiğe uygun davrandığımı, yararlandığım bütün kaynakları atıf yaparak belirttiğimi beyan ederim.

06/06/2018

Başak BİLGİ

ÖZET

Yüksek Lisans Tezi

HİBRİT RESİMLERİ KULLANAN OMUZ SÖRFÜNE KARŞI DİRENÇLİ GRAFİK TABANLI KİMLİK DOĞRULAMA

Başak BİLGİ

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Dr. Öğretim Üyesi Bülent TUĞRUL

Günümüzde en bilinen kimlik doğrulama metodu metin tabanlı şifreler kullanmaktır; fakat bu yöntemle hem güçlü hem de kullanımı kolay şifreler oluşturmak mümkün olamamaktadır. Hem yüksek güvenliğe sahip hem de kolay kullanılabilir bir kimlik doğrulama sistemi tasarımı bilgi güvenliği sistemleri için önemli ve güncel bir problemdir. Grafik şifreler kolay kullanımı ve güvenilir olması nedeni ile klasik metin tabanlı şifreleme yöntemlerine bir alternatif olarak ortaya çıkmıştır. Grafik şifre sistemlerinin çıkış noktası, insanların görsel verileri yazıya ve sayılara göre daha iyi hatırladığı kabuludur. Bu tez çalışmasında kapsamında; ilk aşamada kimlik doğrulama yöntemlerine dair temel kavramlara ve mevcut grafik tabanlı kimlik doğrulama metotlarına yer verilmektedir, ikinci aşamada alternatif grafik tabanlı bir kimlik doğrulama metodu önerilmektedir. Önerilen yöntem önce metin tabanlı bir kimlik doğrulama yöntemi ile kullanıcı deneyimi açısından karşılaştırılmaktadır; sonrasında yöntem omuz sörfüne dirençli olma özelliği kazanıp, tekrar kullanıcı deneyimi ölçülmektedir. Son kısımda ise önerilen grafik tabanlı kimlik doğrulama yöntemi üzerinde hangi geliştirmelerin yapılabileceğine dair önerilere yer verilmektedir.

Haziran 2018, 75 sayfa

Anahtar Kelimeler: Bilgi güvenliği, kimlik doğrulama metotları, grafik tabanlı kimlik doğrulama metotları, grafik şifreler, hibrit resimler, omuz sörfüne dirençli

ABSTRACT

Master Thesis

SHOULDER-SURFING RESISTANT GRAPHICAL PASSWORD AUTHENTICATION USING HYBRID IMAGES

Başak BİLGİ

Ankara University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

Supervisor: Assist. Prof. Dr. Bülent TUĞRUL

Today the most common authentication method is to use text-based passwords; but it is not possible to create strong and easy-to-use passwords using this method. Designing a both high-secure and easy-to-use authentication system is an important and up-to-date problem for information security systems. Graphical passwords have emerged as an alternative to classical text-based encryption methods thanks to the ease of use and reliability. The starting point of graphical password systems is the recognition that people remember visual data better than text and numbers. Within this thesis study; in the first stage concepts related with authentication methods and current graphics-based authentication methods are mentioned; in the second stage an alternative graphics-based authentication method is suggested. The proposed method is initially compared with and a basic text-based authentication method in terms of user experience; after that the proposed method gains the shoulder-surfing resistancy feature, and the user experience is measured again. In the last section, suggestions on what improvements could be made on the proposed graphics-based authentication method are brought up.

June 2018, 75 pages

Key Words: Information security, authentication methods, graphics-based authentication methods, graphical passwords, hybrid images, shoulder-surfing resistant

TEŞEKKÜR

Çalışmalarımı yönlendiren, araştırmalarımın her aşamasında bilgi, öneri ve yardımlarını esirgemeyerek akademik ortamda olduğu kadar insani ilişkilerde de engin fikirleriyle yetişmeme ve gelişmeme katkıda bulunan danışman hocam sayın Yrd. Doç. Dr. Bülent TUĞRUL'a (Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı) tüm içtenliğimle teşekkür ederim.

Çalışmalarım süresince maddi, manevi pek çok fedakârlık göstererek beni destekleyen ve her an yanımda olan anneme ve babama minnettarlığımı belirterek, en derin duygularla teşekkür ederim.

Başak BİLGİ
Ankara, Haziran 2018

İÇİNDEKİLER

KISALTMALAR DİZİNİ

FN	False Negative
FP	False Positive
GB	Gigabyte
MATLAB	Matrix Laboratory
TN	True Negative
TP	True Positive
UML	Unified Modeling Language

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

Bilgisayar biliminin en temel prensiplerinden birisi denetimli erişimdir. Her kullanıcı her bilgisayar kaynağına erişim hakkına sahip değildir, ya da erişimin değişik seviyeleri bulunmaktadır. Günümüzde elektronik ortamda erişim; kullanıcı adı ve alfasayısal şifre kombinasyonu üzerinden sağlanmaktadır. Kayıtlı ve geçerli bir kullanıcı sistemi kullanabilmek için bilgisayara kimliğini ispat etmelidir. Bilgisayar doğru kullanıcı adı ve alfasayısal şifre kombinasyonu girildiğinde kullanıcıyı sistemde doğrular ve kimlik doğrulama başarılı olarak tamamlanır. Kullanıcı ancak bu aşamayı geçtikten sonra sistemde belirlenen işlevleri kullanabilir; örneğin elektronik posta yollamak, ders eklemek, ders bırakmak, para aktarımı gerçekleştirmek, alışveriş yapmak, sosyal medya hesabından paylaşımda bulunmak, ücretli bir oyunu ya da yazılımı kullanmak.

Geçerli bir kullanıcının sistemin olanaklarını kullanmasının dışında sistemde tanımlı olmayan ama sistemi sanki geçerli bir kullanıcıymış gibi kullanmak isteyen kötü niyetli kişiler de olabilmektedir. Bu kişiler kullanıcının alfasayısal şifresini ele geçirmeye çalışabilirler. Kimlik doğrulama bilgisine erişip, bilgisayara bu bilgileri sunan aslında geçerli kullanıcı olmayan bu kişiler de sistemde doğrulanır; fakat bu aslında olmaması gereken bir durumdur; çünkü şifre bilgisi sadece gerçek kullanıcıda ve sistemde bulunmalıdır.

Sistemler kötü niyetli kişilerin alfasayısal şifreleri ele geçirme girişimlerine karşı bazı tedbirler almaktadırlar; fakat alınan tedbirler kimlik doğrulama sürecini zorlaştırmakta veya uzatmaktadır. Bu durumun tam aksine kullanıcılar da daha hızlı ve daha kolay kimlik doğrulama süreci ihtiyaç duymaktadır. Güvenlik ve kullanılabilirlik arasında hep bir ödünleşim olmaktadır. Kullanıcılar genellikle kolay hatırlanan şifreleri seçme eğilimindedirler (Morris ve Thompson 1979, Adams ve Sasse 1999). Bu durumda da oluşturulan alfasayısal şifreler çok kolay bir şekilde kırılabilmektedir. Yakın zamanda yayınlanmış bir makalede büyük bir firmada yapılan bir şifre kırması denemesinden bahsedilmektedir. Firmadaki güvenlik takımı bir şifre kırma yazılımı kullanıp 30 saniye içerisinde çalışanların şifrelerinin %80'ini ele geçirebilmişlerdir (Gilhooly 2005). Bu sebeple hem yüksek güvenliğe sahip hem de kolay kullanılabilir bir kimlik doğrulama

sistemi tasarımı bilgi güvenliği sistemleri için önemli ve güncel bir problemdir. Bu durumla başa çıkabilmek için kullanıcıların güçlü şifreler seçmeleri sistem tarafından zorlanabilir; fakat şifreler güçlü oldukları ölçüde hatırlanmaları da güçleşmektedir. Bu durumda da kullanıcılar şifrelerini not etmek, yazmak gibi güvenlik açısından tehlike oluşturan yöntemlere yönelmektedirler (Kotadia 2005). Şifrelerin belli aralıklarla değiştirilmesi sistem tarafından zorlanabilir; önceden kullanılmış bir şifrenin benzeri ya da aynısının kullanılması da engellenebilir; fakat bu durum da kullanıcının kimlik doğrulama aşamasını güçleştirmektedir. Bunlara ek olarak; kullanıcılar tüm uygulamalarda aynı şifreyi kullanma yoluna gitmektedirler. Her uygulamada aynı şifreyi kullanmanın haklı gerekçeleri vardır; çünkü her uygulama için ayrı şifre oluşturulduğunda daha fazla bilgi hatırlanmak zorunda kalınmaktadır ve kullanıcılar bunu tercih etmemektedirler.

Alfasayısal şifrelerin geliştirici açısından uygulamaya konulması, kullanıcı açısından da kullanımı kolaydır; fakat ihtiyaca cevap verememektedirler. Alfasayısal şifrelerin yetersiz kalmasından dolayı alternatif kimlik doğrulama yöntemleri geliştirilmiştir. Alternatifler içinde jeton tabanlı kimlik doğrulama yöntemleri ile biyometrik tabanlı kimlik doğrulama yöntemleri bulunmaktadır. Jeton tabanlı kimlik doğrulama yöntemlerinde kullanıcı jetonu yanında taşımayı unuttuğunda sisteme giriş yapamamaktadır, biyometrik sistemlerde de kişinin özel bilgileri sistemde tutulmaktadır ve bu tip sistemler sık sık arızalanabilmektedir (Wiedenbeck vd. 2005). Ayrıca jeton tabanlı kimlik doğrulama ile biyometrik kimlik doğrulama yöntemlerinin maliyeti yüksektir (Suo 2006, Bhanushali vd. 2015). Alfasayısal şifrelere diğer bir alternatif de grafik tabanlı şifrelerdir. Grafik tabanlı şifreler de alfasayısal şifreler gibi kullanıcının sahip olduğu bir bilgi üzerinden kimlik doğrulaması yapmaktadırlar. Grafik tabanlı şifrelerin çıkış noktası insanların resimleri sözcüklerden daha kolay hatırlayabildiği kabulüdür. Bu kabul psikoloji biliminde yapılan birçok çalışma ile de desteklenmektedir (Kirkpatrick 1894, Shepard 1967, Paivio 1968, Madigan 2014). Benzer bir çalışmada da ikili kodlama teorisi öne sürülmüştür. Bu teoriye göre metinsel ve görsel bellek farklı hafıza sistemleri tarafından temsil edilmektedirler. Sözlü ifadeler ya da metinle ilişkide oldukları anlamla birlikte temsil edilirken, görsel nesneler kendi anlamını doğrudan gözlemlenerek algıda türetmektedir. Sözlü ifadenin beyin tarafından işlenmesi için

fazladan efor sarfedilmesi gerekmektedir ve bu durum yazılı ifadeyi hatırlamayı daha zor bir kavramsal görev yapmaktadır (Bucci 1985).

Alfasayısal kimlik doğrulama sistemlerinde kullanıcı başka bir uygulamada kullandığı şifreyi yeni bir uygulamada da kullanabilir ama grafiksel kimlik doğrulama sistemlerinde böyle bir ihtimal bulunmamaktadır; çünkü bir resim alfabesi yoktur, her sistem farklı resim kümeleri kullanabilir ve bu durumun doğal sonucu olarak da kullanıcının bir uygulamaya girerken kullandığı şifre elde edilse bile başka birisi başka bir yerde bu bilgiyi kullanamaz. Görsel şifreler daha özelleşmiş sistemlerdir.

Daha özelleşmiş bir yapıda olmasından ve insanın görsel hafızadaki üstünlüğünü denkleme ekleyebildiği için son dönemde görsel tabanlı kimlik doğrulama sistemlerine büyük bir ilgi vardır. Bu tez çalışmasında da benzer bir yönelim bulunmaktadır. İkinci bölümde genel kimlik doğrulama yöntemlerine dair bazı kavramlardan ve ölçütlerden bahsedilmektedir; sonrasında ise mevcut grafik şifre yöntemlerine yer verilmektedir. Üçüncü bölümde öngörülen yöntemde kullanılacak olan hibrit resimlerle ilgili teorik bir altyapı sunulmaktadır. Dördüncü bölümde; ilk aşamada grafik tabanlı şifreler ile alfasayısal şifreleri karşılaştıran bir kullanıcı deneyimi araştırmasına yer verilmektedir. İkinci aşamada öngörülen yeni alternatif grafiksel tabanlı şifre yönteminden bahsedilmektedir. Bu alt bölümde geliştiren görsel şifre tekniğinin teoriksel altyapısı detaylıca anlatılmaktadır. Öngörülen yeni yöntemin uygulama tarafı örnek ekran görüntüleri ile tez içerisinde yer almaktadır. Ekran görüntüleriyle desteklemek suretiyle öngörülen sistem detaylı olarak aşama aşama anlatılmaktadır. Beşinci bölümde öngörülen grafiksel şifre yöntemi ile oluşturulan bir uygulamanın kullanıcılara sunulması sonrasında elde edilen bulgular ortaya konmaktaktadır. Her bir kullanıcı için sonuçlar kaydedilip, üzerinde analizler yapılmaktadır ve yapılan analizler tablolarla, çizelgelerle daha özet bir şekilde anlatılmaya çalışılmaktadır. Elde edilen veriler üzerinde herhangi bir iyileştirme yapılmadan aynen deneyimlendiği haliyle, ham haliyle tez içerisinde yer almaktadır. Son bölümde ise; konuya ilgi duyabilecek araştırmacılar için yöntem üzerinde ne gibi iyileştirmeler yapılabilir, hangi kısımlar üzerinde geliştirme yapılabilir, hangi kısımlarda ne şekilde daha detaylı bir analiz ile daha iyi sonuçlar elde edilebilir gibi fikirlere yer verilmektedir.

Bilgisayar güvenliği hayati önemi olan ve çok güncel bir bilişim konusudur. Bu tez çalışmasında da bilgisayar güvenliğini alternatif, kolay ve sağlam bir yöntem aracılığıyla sağlamak hedeflenmiştir. Tez içerisinde alternatif olarak geliştirilen görsel şifre tekniği kullanılarak ya da üstüne inşaa edilerek uygulamaya geçirilebilir ve bu yeni yöntem grafik tabanlı kimlik doğrulama sistemleri arasında kendine bir yer edinebilir.

2. KAYNAK ÖZETLERİ

Bu bölüm iki alt bölümden oluşmaktadır. İlk altbölümde kimlik doğrulama yöntemlerine dair bazı kavramlardan ve ölçütlerden bahsedilmektedir. Takip eden alt bölümde mevcut grafik tabanlı kimlik doğrulama yöntemlerine değinilmektedir.

2.1 Kimlik Doğrulama Yöntemlerine Dair Kavramlar ve Ölçütler

2.1.1 Yanlış negatiflik, yanlış pozitiflik, doğru negatiflik, doğru pozitiflik kavramları

Bilgisayarlar veri üzerinde iş yaparlar ve veriye güvenmek zorundadırlar. Bilgisayarlara beklenen veri girildiğinde, bilgisayarlar o veriye sahip olan kullanıcının sistemde geçerli bir kullanıcı olduğunu varsayarlar ve o kullanıcının erişimine izin verirler. Beklenen veri girilmediğinde de kullanıcının erişimine izin verilmez. Sisteme giriş denemesinin sonucu ya pozitif olur ya da negatif; fakat iki durumun da alt durumları bulunmaktadır. Sisteme giriş başarılıysa; bilgiyi sisteme geçerli bir kullanıcı girmişse bu durum "doğru pozitiflik" olarak, bilgi sisteme aslında geçerli olmayan bir kullanıcı tarafından girilmişse de ortaya çıkan durum "yanlış pozitiflik" olarak adlandırılır. Kendi elektronik posta hesabına şifresiyle başarılı bir şekilde giriş yapan kişinin durumu "doğru pozitiflik"tir. Başkasının elektronik posta hesabına tahmin yöntemiyle elde ettiği şifreyle girmeye çalışan ve bu girişiminde başarılı olan birisinin durumu da "yanlış pozitiflik"tir. İki durumda da sisteme giriş başarılı olmuştur. Sisteme giriş başarısız olduğunda ise iki alt durum vardır; bilgiyi sisteme geçerli bir kullanıcı girmişse ve kimlik doğrulama başarısızsa bu durum "yanlış negatiflik" olarak, bilgiyi sisteme geçersiz bir kullanıcı girmişse ve kimlik doğrulama yine başarısız ise bu durum da "doğru negatiflik" olarak adlandırılır. Geçerli bir kullanıcının beklenen bilgiyi sisteme girememesine örnek olarak şifresini unutan bir öğrencinin okulun öğrenci işleri sistemine girip notlarını öğrenememesi verilebilir. Diğer duruma örnek olarak da; başkasının e-posta hesabına girme denemesi yapan bir kullanıcının kimliğinin sistemde doğrulanamaması verilebilir.

2.1.2 Kaba kuvvet saldırısı

Mümkün olan bütün şifre kombinasyonlarının denenmesine kaba kuvvet saldırısı denir. Bu en çok zaman alan ve en zor olan saldırı çeşididir. Alfasayısal şifreler; boşluk karakterini hesaba katılmazsa ve şifre uzunluğu N olarak alınırsa 94^N şifre uzayına sahiplerdir (Suo vd. 2005). Grafik tabanlı şifrelerde sonsuz bir şifre uzayı elde etmek mümkündür. Şifre uzayının büyümesi grafik tabanlı şifrelere kaba kuvvet saldırısı yapmanın güçleşmesini sağlamaktadır.

2.1.3 Sözlük saldırısı

Sözlük saldırısında; saldırgan çok fazla kullanılan şifreleri ve kullanılması muhtemel şifreleri; kullanımı yaygın olan şekillerde formülize ederek kendisine bir kelime haznesi oluşturur. Saldırgan her şifre kombinasyonunu denemektense belli bir şifre kümesi üzerine yoğunlaşır. Örneğin 8 karakterlik ama ilk bakışta hiçbir şekilde akılda bir kalıcılığı olmayan şifreleri örneğin "Dtyd%2Sg", "Rstu%63W" elemiş olur; kullanıcıların bu tip şifreleri kullanmayı tercih etmediği kabulunden yola çıkarak daha olası ihtimaller örneğin "Ankara06%", "Artvin08%" üzerinden saldırısını gerçekleştirir. Sözlük saldırısı; kaba kuvvet saldırısına kıyasla daha az sayıda kombinasyonu deneyerek şifreyi kırmaya çalışır. Alfasayısal şifreler sözlük saldırısına karşı savunmasızdır. Sözlük saldırısı ile kaba kuvvet yaklaşımdan çok daha kısa sürede şifreler kırılabilmektedir; çünkü alfasayısal şifrelerde şifre uzayı 94^N olarak hesaplansa da pratikte kullanılan şifre uzayı çok daha küçüktür (Bagchi ve Atluri 2006). Grafik tabanlı şifrelerde sözlük saldırısı yapmak alfasayısal şifrelere göre daha zordur; çünkü herhangi bir kombinasyonun başka bir kombinasyona göre daha seçilebilir olduğu bir grafik tabanlı şifre yöntemi seçilmemişse; teoride öngörülen grafik tabanlı şifre uzayı ile pratikte kullanılan arasında çok fark olması için herhangi bir sebep yoktur.

2.1.4 Sosyal mühendislik

Bir kullanıcının telefon görüşmesi dinlenerek şifresi ele geçirilebilir, ya da bir kâğıda yazılan bir şifre bir yabancının eline geçebilir ya da bir dolandırıcılık sitesi kurulup kullanıcıların şifreleri toplanabilir. Başka bir yöntemde ise kullanılan bir bankanın ya da alışveriş sitesinin uzantısına sahip olan sahte bir elektronik posta yollanarak, kullanıcıdan şifresini girmesi talep edilip, şifre ele geçirilebilir. En kolay şifre saldırısı bu sahte elektronik posta yöntemidir.

2.1.5 Tahmin yöntemi

Tahmin yöntemiyle de şifreler ele geçirilebilir; örneğin kişinin doğum yeri ve tarihi bilgisi gibi veriler çeşitli kombinasyonlarla denenerek şifresi kırılabilir. Günümüzde sosyal medyanın da yaygınlaşması ile kişisel veriler daha ulaşılabilir bir hal almıştır. Örneğin; kullanıcının internet bankacılığı ortamındaki gizli sorusunun cevabı sosyal medya paylaşımlardan yola çıkılarak bulunabildiği durumlar meydana gelebilmektedir. Kullanıcılar sosyal medyada şahsi bilgilerini gönüllü olarak paylaşmaktadırlar; kötü niyetli kimseler sosyal medya hesaplarını takibe alıp kullanıcıların şifreleriyle ilgili tahminlerde bulunabilirler. Alfasayısal şifrelerde tahmin yöntemi ile şifrelerin ele geçirilmesi çok rastlanan bir durumdur. Grafik tabanlı şifrelerde de tahmin yöntemi ile şifreler ele geçirilebilir; fakat tahmin yöntemi ile yapılabilecek bir şifre saldırısı ile ilgili detaylı ve bulgulardan yola çıkan bir genel bir yargıya varılması mümkün görünmemektedir. Geliştirilmiş olan grafik tabanlı şifrenin doğası incelendikten sonra ilgili teknikte oluşturulan şifrelerin tahmine açık olup olmadığına dair bir yorum yapılabilir.

2.1.6 Casus yazılımlar

Kullanıcının bilgisayarına klavyesini izleyen bir yazılım monte edilerek de kullanıcının alfasayısal şifresi ele geçirilebilir ya da kullanılan bir yazılım içerisine kullanıcının şifrelerini bir sunucuya periyodik olarak yollayan ajan programlar monte edilmek

suretiyle de alfasayısal şifreler elde edilebilir. Aynı tip bir saldırıyı grafik şifrelerde uygulamak genel olarak mümkün değildir; çünkü grafik şifreler klavye yerine daha çok fare hareketleri ve tıklamaları ile kimlik doğrulama yapma eğilimdedirler. Klavye tuşlarını kullanmayan grafik tabanlı bir şifre tekniğinde saldırı yapanın elinde sadece fare hareketleri ve tıklamaları bulunacaktır; bu veriler üzerinden de şifreyi ele geçirebilmesi mümkün değildir. Bu verilerin tıklamayı yorumlayacak olan programın uygulama bilgisi, pencerenin konumu, boyutu ve zamanlama bilgisi ile birleştirilmesi gereklidir; ancak diğer bilgiler de elde edilirse bir yorum yapılabilir.

2.1.7 Omuz sörfü

Omuz sörfü; kullanıcı adı, şifre veya çok özel bilgiler yazılırken ya da erişim kısıtlı sistemlere erişilirken kullanıcının izlenmesidir. Omuz sörfü yöntemiyle de alfasayısal şifreler ele geçirilebilir. Omuz sörfü yöntemi grafik tabanlı şifreler için de geçerlidir; fakat omuz sörfü yöntemi ile yapılabilecek bir şifre saldırısı ile ilgili detaylı ve bulgulardan yola çıkan bir genel bir yargıya varılması aynen tahmin yöntemindeki gibi henüz mümkün görünmemektedir. Geliştirilmiş olan grafik şifrenin doğası incelendikten sonra ilgili teknikte oluşturulan şifrelerin omuz sörfüne imkan verip vermediğine dair bir yorum yapılabilir.

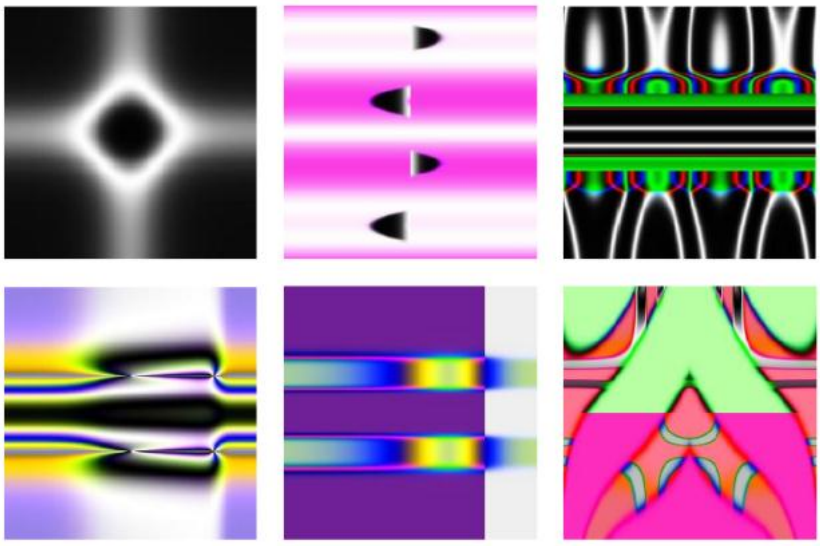
2.1.8 Tanıma tabanlı ve anımsama tabanlı grafiksel kimlik doğrulama kavramları

Grafik tabanlı kimlik doğrulama sistemleri “tanıma tabanlı” ve “anımsama tabanlı” olmak üzere iki ana kategori altında toplanmıştır. Tanıma tabanlı grafiksel kimlik doğrulama sistemlerinde; kullanıcı kayıt olurken bir resim kümesi üzerinden şifresini temsil etmek üzere seçimler yapar, sisteme giriş yaparken ise kayıt olurken seçtiği resimleri tüm resim kümesi içerisinden tanınmaya çalışır. Tanıma işlemi başarı ile biterse kullanıcının kimliği sistemde doğrulanır. Anımsama tabanlı grafiksel kimlik doğrulama sistemlerinde ise; kullanıcıdan kayıt olurken ürettiği grafiksel bir çalışmayı tekrar üretmesi istenir. Kullanıcı her sisteme girişinde aynı grafiksel çıktıyı üretirse kullanıcının kimliği sistemde doğrulanır.

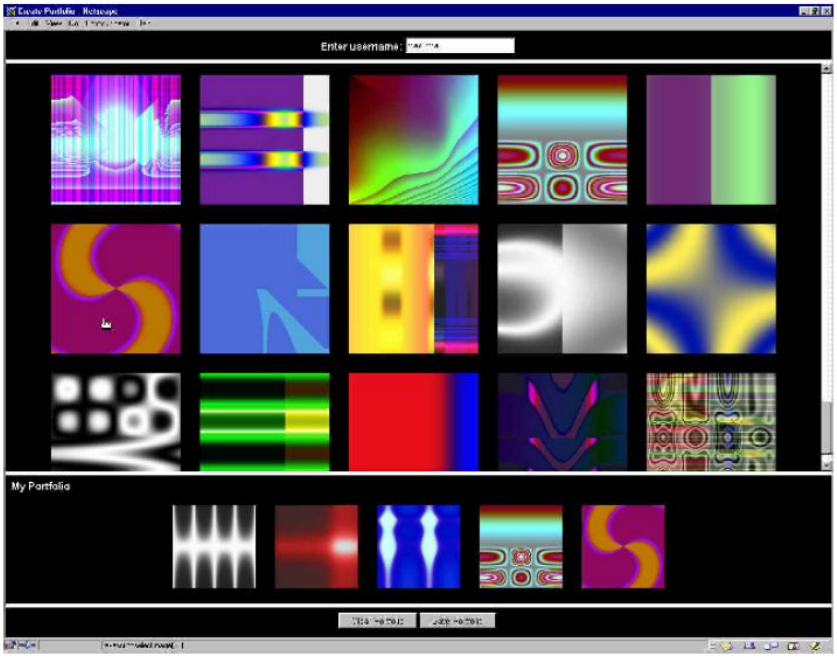
2.2 Mevcut Grafik Tabanlı Kimlik Doğrulama Yöntemleri

2.2.1 Rastgele oluşturulan soyut resimleri kullanma yöntemi

Rastgele üretilen bir rakam kümesinden soyut bir resim üretme tekniği (hash visualisation) Perrig ve Song (1999) tarafından geliştirilmiştir. Şekil 2.1'de bu teknikle oluşturulan soyut resimlerden bazı örnekler bulunmaktadır. Dhamija ve Perrig (2000) üretilen soyut resimleri kullanarak tanıma tabanlı bir kimlik doğrulama yöntemi tasarlamışlardır. Tasarladıkları yöntemde şekil 2.2'de görüldüğü üzere; kullanıcıdan bu teknik ile oluşturulmuş olan soyut resim arşivinden belirlenmiş bir sayıda seçim yaparak kendi portfolyosunu oluşturması istenir. Kullanıcı sisteme erişmek istediğinde kendisine soyut resim arşivinden kendi portfolyosundan resimleri de bulunduran bir resim kümesi sunulur. Kendi portfolyosuna ait olan resimleri tanıyabilen kullanıcının kimliği sistemde doğrulanır. Kimlik doğrulamada kullanılan resimlerin kendileri veri tabanında tutulmaz, resimlere ait çekirdek (seed) değerler tutulur ve çekirdek değer 8 bayt büyüklüğündedir. Tutulan çekirdek değer kullanılarak resim tekrar üretilebilmektedir.



Şekil 2.1 Rastgele oluşturulan soyut resimleri kullanma yöntemi ile üretilen resimler (Dhamija ve Perrig 2000)



Şekil 2.2 Resim portfolyosu oluşturma ekranı (Dhamija ve Perrig 2000)

Bu yöntemde; çizelge 2.1'de görülebileceği gibi kullanıcının hem şifresini oluşturma süresi hem de sistem tarafından doğrulanma süresi geleneksel yaklaşıma oranla artmıştır.

Çizelge 2.1 Rastgele oluşturulan soyut resimleri kullanma tekniği ile üretilen şifreler ile metin tabanlı şifrelerin oluşturulma ve sisteme giriliş sürelerinin karşılaştırılması (Dhamija ve Perrig 2000)

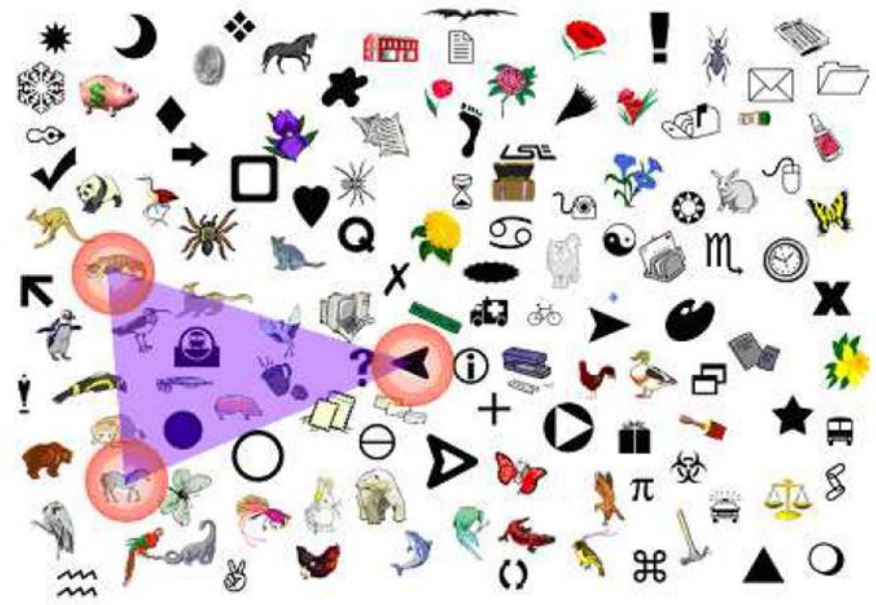
	Metin Tabanlı Şifre	**Hash Visualisation Tekniği İle Üretilen Şifre**
Oluşturma Süresi	25	45
Sisteme Giriş Süresi	18	32
Sisteme Giriş Süresi (Bir Hafta Sonra)	24	36

Bu yöntemde parola uzayı; N veri tabanındaki resim sayısı, K portfolyodaki resim sayısı olmak üzere N!/K!(N-K)!'dir (Suo vd. 2005). 20 resim arasından 5 seçim yapıldığı bir örneklemde parola uzayı 15504 olarak hesaplanır. Bu değer 4 haneli alfasayısal bir

şifrenin parola uzayı olan 10000'den büyüktür. Resim sayısı arttırılarak parola uzayı genişletilebilir; fakat bu seçim de yanlış negatiflerin artmasına neden olabilmektedir; çünkü sistemde geçerli bir kullanıcı çok fazla resim olduğunda karışıklık yaşayacaktır. Bu durum da kullanıcıda bıkkınlığa ve zaman kaybına neden olabilme ihtimaline sahiptir. Ayrıca şifrelerin sistemde arka planda düz metin olarak tutuluyor olması da öngörülen tekniğin zayıf bir yönüdür.

2.2.2 Dışbükey örtü yöntemi

Dışbükey örtü (convex hull) yöntemi Sabroda ve Birget (2002) tarafından omuz sörfü problemine çözüm getirmek amacıyla geliştirilmiştir. Tekniklerinin ana çıkış noktası kimlik doğrulama süreci herhangi bir cihazla kaydedilse bile şifrenin ele geçirilememesidir. Kayıt aşamasında kullanıcıya çeşitli nesnelerin resimleri sunulur, kullanıcı bunlardan belirlenmiş sayıda seçim yapar ve bu nesnelerin her birisi kullanıcının geçiş nesnesi (pass-object) olarak sistemde saklanır. Kullanıcı sistemde doğrulanmak istediğinde önceden belirlemiş olduğu geçiş-nesnesi kümesinden bazı nesneleri de içeren bir resim gösterilir.



Şekil 2.3 Kullanıcının seçtiği nesnelerin oluşturduğu dışbükey örtü (Sabroda ve Birget 2002)

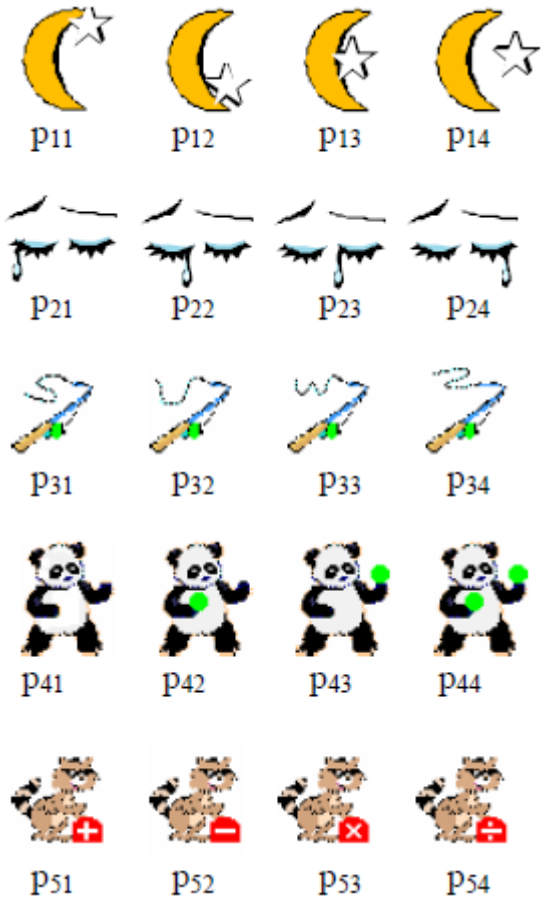
Şekil 2.3'de gösterildiği gibi kullanıcı kendi seçtiği resimleri tanıyıp, bu resimlerin oluşturduğu dışbükey örtünün içerisindeki herhangi bir alana tıklandığında başarılı olur. Sabroda ve Birget (2002) şifrenin tahmin edilmesini zorlaştırmak için kimlik doğrulama ekranında 1000 nesne kullanmayı düşünmüşlerdir; fakat 1000 nesne kullanınca görüntü çok kalabalık bir hal almaktadır, nesneler neredeyse ayırt edilemez olmaktadır. Öte yandan çok az sayıda nesne kullanımı da parola uzayının küçülmesine neden olmaktadır ve bu durum nesnelerin oluşturduğu dışbükey örtünün fazla büyümesine neden olmaktadır. Dışbükey örtünün büyümesi de şifrenin tahmin edilebilirliğini arttıran bir faktör olmaktadır. Bu yaklaşımdaki zayıflık; rastgele tıklama sonucu sistemde tanımlı olmayan birisi doğru alana tıkladığında sistem tarafından doğrulanabilir. Bu problemi aşmak için süreç birkaç kere tekrarlanabilir; böylelikle yanlış pozitiflerin sayısı azaltılabilir; fakat bu durum geçerli bir kullanıcıda bıkkınlığa ve zaman kaybına neden olabilme ihtimaline sahiptir.

2.2.3 Resimlere atanan kodları klavyeden giriş yöntemi

Man vd. 2003'de omuz sörfü problemine çözüm odaklanmış bir grafiksel kimlik doğrulama tekniği geliştirmişlerdir. Bu yaklaşımda kullanıcı birçok geçiş nesnesi (pass-object) arasından seçimler yapar. Şekil 2.4'de görüldüğü üzere oluşturulan her geçiş nesnesi kümesinin her üyesinin eşit sayıda değişik biçimi vardır ve her biçimin eşsiz bir kodu vardır. Her nesneye denk gelen p_{ij} değeri kullanılan algoritmaya göre değişiklik gösterir.

Kimlik doğrulama esnasında kullanıcıya kendi geçiş nesnesi kümesinden de elemanlar bulunduran birçok nesne içeren bir ekran sunulur. Sunulan ekranda geçiş-nesnesi kümesinin elemanları herhangi bir biçimde olabilir. Kullanıcı sistemde doğrulanmak için ekranda kendi geçiş nesnesi kümesinden elemanlara tekabül eden kodları sırasına uygun olarak klavyeden metin olarak girer. Bu kod kümesinin başına bir bilgi daha girmesi istenir o da kullanıcının gözlerinin geçiş nesnesi kümesinin elemanlarının ne tarafında kaldığı bilgisidir. Kullanıcı, iki gözü de geçiş nesnesi kümesinin oluşturduğu alanın dışında ise c_1, iki gözü de bu alanın içinde ise c_2, sadece sol gözü içerde ise c_3,

sadece sağ gözü içerde ise c_4 girmelidir. Her duruma denk gelen c_i değeri kullanılan algoritmaya göre değişiklik gösterir.



Şekil 2.4 Geçiş nesnesi kümesi elemanlarının değişik biçimleri (Man vd. 2003)

Şekil 2.5'de bir kimlik doğrulama ekranı örneği görülmektedir. Bu ekranda kullanıcı:

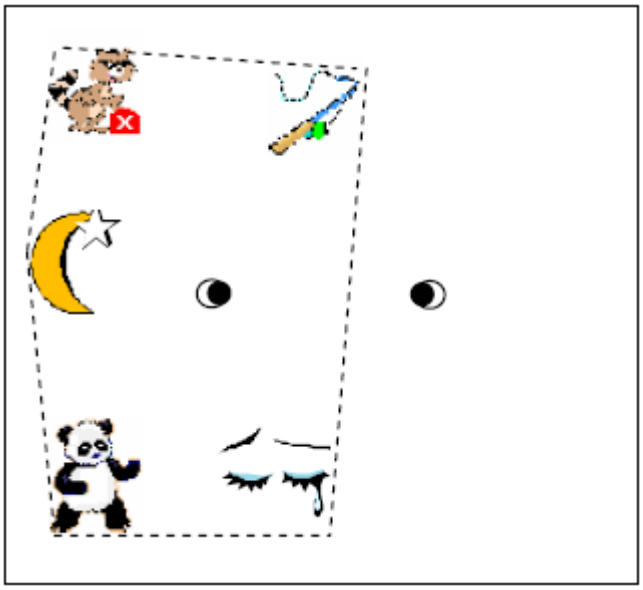
$$p_{11}, p_{24}, p_{32}, p_{41}, p_{53}$$

nesnelerini tanır ve sonrasında nesnelerin göze göre konumunu belirler. Kullanıcının gözlerinin konumu bu kimlik doğrulama ekranında c_3'e tekabül etmektedir. Kullanıcı bu bilgiyi de nesnelerin bilgisinin başına ekler ve şifresini $(c_3, p_{11}, p_{24}, p_{32}, p_{41}, p_{53})$ olarak belirler. Bu örnekte:

$$c_i=i^2$$

$$p_{ij}=i+j$$

olarak alınırsa, kullanıcının sisteme metin olarak 926558 girmesi beklenir, ve girdiği takdirde kullanıcının sistemde kimliği doğrulanır.



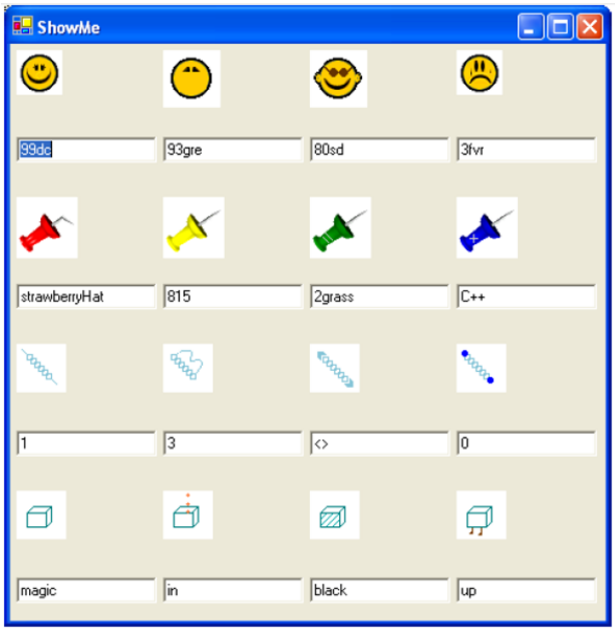
Şekil 2.5 Resimlere atanan kodları klavyeden giriş yönteminde kimlik doğrulama ekranı (Man vd. 2003)

Bu teknik, tüm kimlik doğrulama süreci kaydedilse bile kullanıcının şifresini ele geçirmenin çok zor olduğu iddiasındadır; buna dayanak olarak da herhangi bir fare tıklaması olmamasını göstermektedir. Her geçiş nesnesi kümesi elemanına denk gelen p_{ij} değerlerini hesaplamak yerine ezberlemek yöntemi diğer bir seçenek olan tek tek hesaplama yöntemine oranla kullanıcıya daha kolay gelebilir; fakat her iki seçenekte de kullanıcı rahat ve hızlı bir kimlik doğrulama deneyimlememektedir. Hem resimlerin hem de kodların ezberlenmesi tekniğin kullanılabilirliğini azaltmaktadır.

Bu tekniğin parola uzayı alfasayısal şifrelerle aynıdır; çünkü tüm süreç sonunda yine sisteme alfasayısal bir şifre girilmektedir. Alfasayısal şifrelerde yaşanan problemlerin aynısı bu yaklaşımda da bulunmaktadır. Ezber içermesi sistemin eksi bir yönüdür.

2.2.4 Resimlere atanan kişisel kodları klavyeden giriş yöntemi

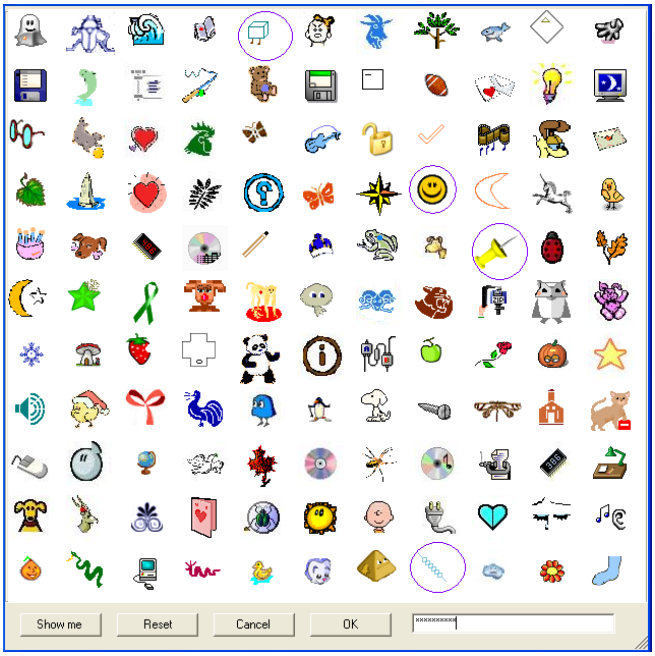
Hong vd. (2004), Man vd. (2003) tarafından geliştirilen yöntem üzerinde bazı iyileştirmeler yapılabileceğini öngörmüşlerdir. Hong vd. (2004) şekil 2.6'da görüldüğü üzere geçiş nesnesi kümesinin elemanlarına atanan kodların kullanıcı tarafından belirlenmesine izin vermişlerdir.



Şekil 2.6 Kullanıcın nesnelere kendi belirlediği kodları ataması ekranı (Hong vd. 2004)

Kullanıcı burada gülen yüze karşılık 1999 yılında doktorasını aldığı ve mutlu bir anı olarak hatırladığı için '99dc' değerini, ateşli yüze karşılık 3 yaşında yüksek ateş hastalığı geçirdiği için "3fvr' değerini atamıştır.

Şekil 2.7'deki gibi bir kimlik doğrulama ekranı geldiğinde kullanıcı kendi geçiş nesnesi kümesine ait olan nesneleri tespit eder ve onlara karşılık gelen kendisinin önceden belirlemiş olduğu kodları metin olarak girerek sistemde doğrulanır. Bu örnekte üretilen şifre "99dc8151up"tır.

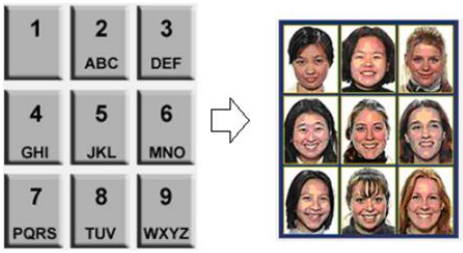


Şekil 2.7 Resimlere atanan kişisel kodları klavyeden giriş kodları yönteminde kimlik kimlik doğrulama ekranı (Hong vd. 2004)

Önceki yaklaşımda olduğu gibi yine son aşamada alfasayısal bir şifre oluşturulduğu için bu teknikte de parola uzayı alfasayısal şifrelerin parola uzayı ile aynıdır ve yine alfasayısal olduğu için bu teknik alfasayısal şifrelerin eksikliklerine ve dezavantajlarına sahiptir.

2.2.5 Yüzleri şifre olarak kullanma yöntemi

Yüzleri şifre olarak kullanma tekniği Real User Corporation tarafından geliştirilmiştir (http://www.realuser.com 2005).



Şekil 2.8 Tuşların yerini yüzlerin alması kodları alması (http://www.realuser.com 2005)

Bu teknikte; kullanıcı şekil 2.8'de görüldüğü gibi tuşlara tıklamak yerine yüzlere tıklar.

Şekil 2.9 Geçiş yüzü yönteminde kimlik doğrulama ekranı (http://www.realuser.com 2005)

Kayıt aşamasında kullanıcı geçiş yüzü (passface) veri tabanından 4 adet geçiş yüzü seçer; bu 4 yüz artık onun geçiş yüzü kümesi olur. Şekil 2.9'da görüldüğü üzere kimlik doğrulama aşamasında kullanıcıya kendi seçtiği yüzlerden birini de içeren 9 adet yüz içeren çizgilerle ayrılmış bir resim gösterilir. Kullanıcı bu 9 resim arasında kendi geçiş yüzü kümesinin elemanı olan resmi tanır ve o resmin herhangi bir yerine tıklar ve sonraki aşamaya geçer. Sonraki aşamada da yine aynı işlem yapılır. Birçok kez bu işlem tekrarlandıktan sonra kullanıcının kimliği sistemde doğrulanır. Bu teknik insanların yüzleri resimlerden daha iyi tanıdığı fikrinden yola çıkmıştır (Suo vd. 2005). Valentine'ın (1999) yaptığı araştırmalara göre bu teknikte geçiş yüzü nesneleri kümesinin elemanları uzun zaman aralıkları sonrasında bile hatırlanabilmektedir. Brosstoff ve Sasse'nin (2000) çalışmalarında da bu teknikteki yanlış negatif oranının, bu yöntem 1/3 oranla kullanılmasına rağmen, 1/3 olduğunu tespit etmişler. Yapılan çalışmalarda geçiş yüzü tabanlı kimlik doğrulama sürecinin alfasayısal kimlik doğrulama sürecine göre daha uzun sürede tamamlandığını ortaya konmuştur (Valentine 1998). Bu teknikle oluşturulan şifreler incelediklerinde, şifreler arasında ortak örüntüler elde edilmiştir (Davis vd. 2004). Örneğin kullanıcıların genellikle kendileriyle aynı

etnik kökenden olan yüzleri seçtiği tespit edilmiştir. Bu problem geçiş yüzü kümelerinin oluşturulmasını kullanıcının seçimine bırakmayarak aşılabilir; fakat bu durum da kullanıcıların şifrelerini hatırlamasını zorlaştırma potansiyeline sahiptir.

2.2.6 Mini resimlere tıklama yöntemi

Sadece mobil cihazlarda kullanılabilen bir grafiksel kimlik doğrulama mekanizması geliştirilmiştir (Jansen 2004). Bu yöntemde şekil 2.10'da görüldüğü üzere kullanıcı sisteme kayıt olurken 30 sayıda mini resimden (passcode) oluşan mobil cihazın ekranı ile aynı büyüklüğe sahip bir tema ya da resim seçer. Bu resim üzerinde sırasını aklında tutarak resimlerin üzerine tıklamak yoluyla şifresini oluşturur. Kimlik doğrulama esnasında kullanıcı kayıtta seçtiği resimleri doğru sırada sisteme girer. Bu tekniğin bir dezavantajı şifre alanının küçük olmasıdır; çünkü mobil cihazlarda ekran küçüktür ve dolayısıyla 30'dan fazla resim sığmamaktadır. Parola uzayı bu sebeple K şifre uzunluğu olmak üzere 30^K'dır (Jansen 2004). Parola uzayını büyütmek için art arda tıklamalara izin verilmesi önerilmiştir. Tek tıklamalara, çift tıklamalar da eklendiğinde parola uzayı:

$$(30+(30*30))^K=930^K$$

olarak genişleyebilmektedir. Bu yaklaşımdaki parola uzayı alfasayısal şifrelerin parola uzayı ile karşılaştırıldığında tablodaki sonuçlar elde edilmiştir. (Jansen 2004).

Şekil 2.10 Mini resimlere tıklama yönteminde kimlik doğrulama ekranı (Jansen 2004)

Çizelge 2.2 Mini resimlere tıklama yönteminde oluşturulan şifre uzunluğu ile metin şifresi uzunluğunun karşılaştırılması (Jansen 2004)

Metin Şifresinin Uzunluğu	6	7	8	9	10	11	12
Mini Resimlerden Oluşan Şifrenin Uzunluğu	4	5	6	6	7	7	8

Çizelge 2.2'ye göre bu yaklaşımla oluşturulmuş 4 uzunluğundaki bir şifrenin parola uzayı 6 karakter uzunluğundaki alfasayısal bir şifre ile oluşturulan parola uzayı ile eşittir. Çift tıklama yöntemi kullanıcı açısından sisteme giriş esnasında karmaşık bir durum yaratabilir; bu açıdan çift tıklama olan seçeneği kullanmamak daha doğru bir tercih olabilir. Bu durumda da şifre uzayı küçülecektir.

2.2.7 Bir sır çiz yöntemi

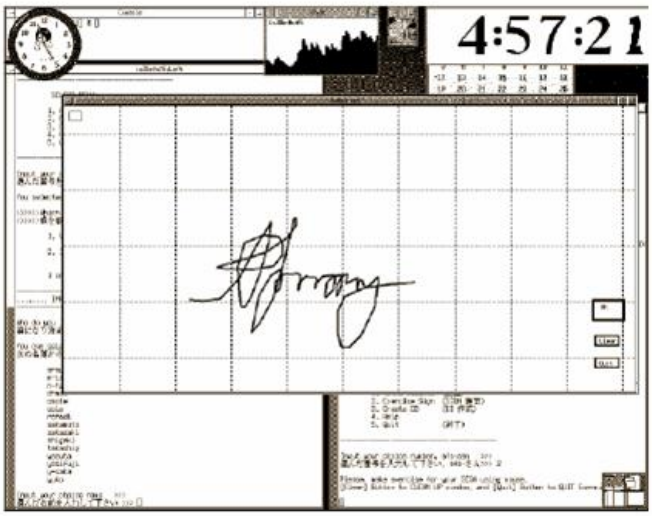
Adından da anlaşıldığı üzere bu teknikte kullanıcı sisteme kayıt olurken şekil 2.11.a'da görüldüğü üzere bir çizim yapar. Bu teknik; kullanıcının kendi eşsiz şifresini kendisinin yaratabilmesine izin vermek amacıyla geliştirilmiştir (Jermyn vd. 1999). Şekil 2.11.a'da görüldüğü üzere kullanıcı bir sır çizmiştir. Çizim esnasında kullanılan hücreler, kullanılma sıralarıyla birlikte saklanır. Kimlik doğrulama esnasında şekil 2.11.b'de görüldüğü üzere kullanıcı bu şekli bir daha çizer. Burada dikkat edilen husus aynı hücrelerin aynı sırayla kullanılmasıdır. Kullanıcı çizim işlemini bitirdikten sonra şekil 2.11.b'deki gibi bu hususlara göre yapılan çizim kontrol edilir; çizim başarılı ise kullanıcının kimliği sistemde doğrulanır; değilse şekil 2.11.b'de görüldüğü üzere kimlik doğrulama işlemi başarısız olur ve şekil 2.11.c'deki gibi sırrın tekrar çizilmesi beklenir. Bu teknikte parola uzayı alfasayısal şifrelere oranla çok daha büyüktür (Jermyn 1999). Bu yöntemle oluşturulan şifrelerin tahmin edilebilirlikleri araştırılmıştır (Thorpe ve Oorschot 2004). Araştırmalar sonucunda çizimlerin başlangıç ve bitiş noktaları arasında her hangi bir tahmin edilebilirlik bulunamamıştır; fakat belirgin simetriler yakalanmıştır; örneğin çarpıların, dikdörtgenlerin, harflerin ve sayıların kullanıldığı gözlemlenmiştir. Bu çalışma şunu göstermiştir ki kullanıcılar tahmin edilebilir karakteristiklere sahip şifreler seçmektedirler. Tekniğin bir diğer zayıf noktası da kullanıcının her seferinde aynı hücreleri aynı sıra ile kullanarak aynı çizimi üretmesinin beklenmesidir; bu durum da yanlış negatife düşen kullanıcı sayısının yüksek olmasına sebep olabilecek bir faktördür.

Şekil 2.11.a. Kayıt, b. Giriş, c. Kontrol (Jermyn vd.1999)

Bir diğer zayıf noktası da bu yöntemde çapraz çizgileri çizmek zordur bir hücre çizgisine yakın geçen çizimler varsa kullanıcı şifresini girerken zorlanacaktır. Bir başka sorun yaratabilecek durum da kullanıcı hücreleri ayıran çizgilere ve kesişimlere yakın çizimler yaparlarsa arka planda çalışan algoritma, sistemin neyi kastettiğini doğru bir şekilde anlamlandıramayabilir.

2.2.8 İmza yöntemi

Şekil 2.12'de görüldüğü üzere kimlik doğrulama esnasında kullanıcıdan imzasını atmasını isteyen bir sistem tasarlanmıştır (Syrukri vd. 1998). Bu teknikte imza fare kullanılarak atılmaktadır. Kayıt aşamasında kullanıcıdan imzasını atması istenir. Sonrasında sistem imza alanını tüm alandan çıkarır, alanı büyütür, küçültür veya gerekirse döndürür. Normalizasyon işleminden sonra elde edilen imza bilgisi veri tabanına yazılır. Sonrasında kullanıcıdan bir kez daha imza atması istenir, bu aşamada yine normalizasyon işlemi uygulanır ve sonrasında imzanın parametreleri elde edilir. Bu parametreler imza uygulaması içerisinde saklanır.



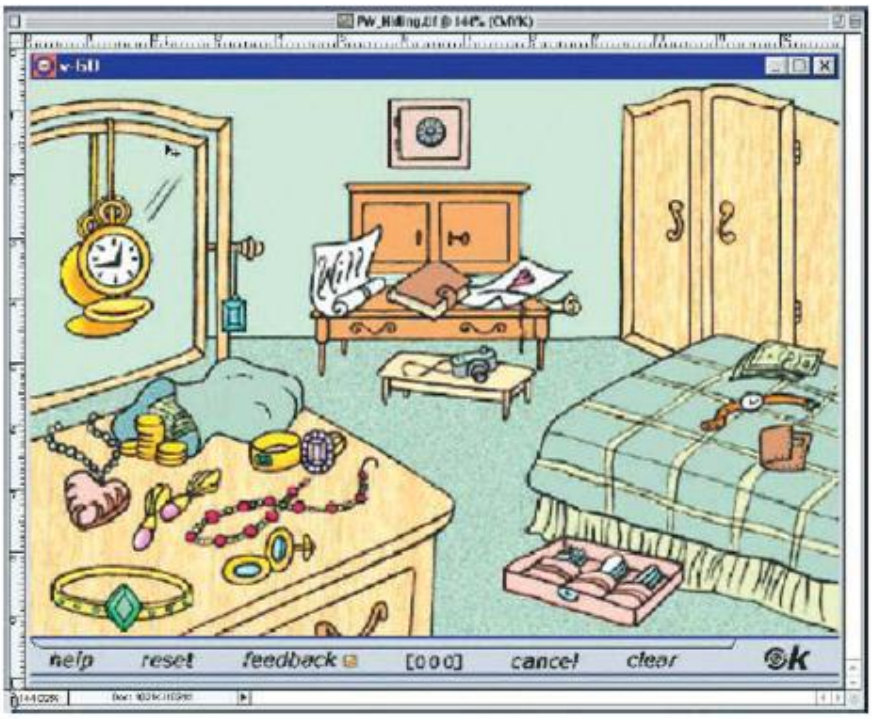
Şekil 2.12 İmza atma ekranı (Syrukri vd. 1998)

Bu yaklaşımda kullanıcının herhangi bir bilgiyi ezberlemesi gerekmemektedir. Bu tekniğin en güçlü yanı güçlü şifreler oluşturulmasını sağlamasıdır; çünkü kişinin imzasını taklit etmek fazlasıyla zordur. Bu teknikte parola uzayı da sonsuz olarak

görülmektedir. (Suo vd. 2005) Her kullanıcı fare kullanımında seri ve rahat olamayabilir, bunun için bu tekniği kullanacak cihazların özel bir dokunmatik kalem benzeri ek bir donanım kullanmaları kullanıcı deneyimini kolaylaştırabilir. Bu tekniğin zayıf noktası arka planda çok iyi çalışan bir imza tanıma algoritmasına ihtiyaç duymasıdır; fakat imza tanıma algoritmalarının uyarlanması oldukça güç bir işlemdir. Dokunmatik özel bir kalem kullanılması da sisteme fazladan bir maliyet getirmektedir.

2.2.9 Resim üzerinde belirli alanlara tıklama yöntemi

Blonder (1996) bir resim üzerinde belirli alanlara tıklamak suretiyle kimlik doğrulama işlemi yapan bir sistem tasarlamıştır.



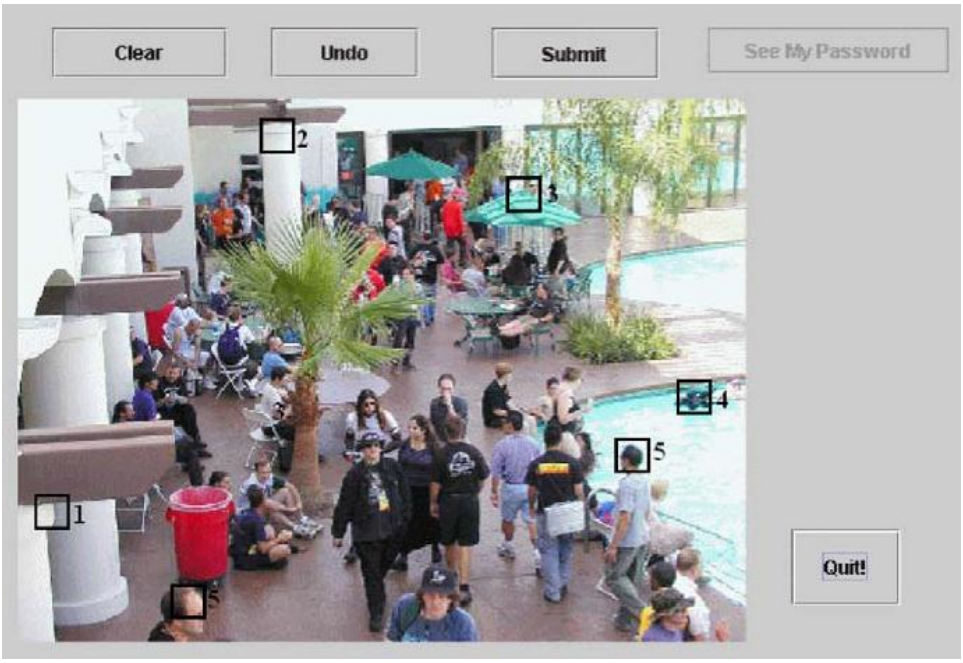
Şekil 2.13 Passlogix kimlik doğrulama ekranı (http://www.passlogix.com 1996)

Bu teknikte kimlik doğrulama esnasında kullanıcı tam olarak belirlenen alanlara tıklamalıdır. Passlogix firması Blonder'ın (1996) fikrini temel alan bir grafiksel kimlik doğrulama yöntemi geliştirmiştir. Şekil 2.13'de görülen bir Passlogix firmasına ait uygulamada kullanıcı resim üzerinde birçok nesneye tıklar.

Bu yöntenmde nesneler arasında görünmeyen sınırlar tanımlanmıştır bu sınırlara göre hangi nesneye tıklandığı sistem tarafından algılanır. Nesneler arasındaki tıklamalar bir hikâye anlatır gibi kurgulanabilir. Örneğin bir mutfak resminde kullanıcı birçok aşamayı içerecek şekilde meyve salatası hazırlayabilir. İlk aşamada meyvelere tıklar sonra meyveleri yıkamak için çeşmeye tıklar sonra bir tabak alır ve yıkanmış meyveleri içine koyar, sonrasında bıçağa tıklar ve sonrasında çatala tıklar. Meyve salatası yenmeye hazır halde geldiği anda kullanıcının kimliği sistemde doğrulanmış olur. Bu yaklaşım diğer yaklaşımlara oranla ilk olmasının da getirdiği avantaj ile büyük bir kullanıcı kitlesine ulaşmıştır, daha çok tanınabilmiştir ve sonrasında Oracle Corporation tarafından satın alınmıştır.

2.2.10 Resim üzerinde istenen alanlara tıklama yöntemi

Wiedenback vd. (2005) tarafından geliştirilen bu yöntem Blonder'ın (1996) fikri üzerine inşaa edilmiştir. Yöntemi sistemde rastgele resimlerin de kullanılmasına izin vererek genişletmişlerdir. Sonuç olarak bu yöntemde kullanıcı Blonder'ın (1996) tasarladığı yöntemden farklı olarak resim üzerinde her hangi bir yere tıklanmasına izin vermektedir. Kayıt aşamasında kullanıcı istenen sayıda tıklama yaparak kendi geçiş noktası (passpoint) kümesini oluşturur. Geçiş noktası kümesinin elemanlarının piksel koordinatları, tıklanma sıralarına göre sistemde saklanır. Şekil 2.14'de görülen kimlik doğrulama ekranında kullanıcı sırayla hatırladığı geçiş noktası kümesi elemanlarına tıklar; kullanıcının tıkladığı alanlar karışıklığa sebebiyet vermemek amacı ile kutucuk içerisine alınır ve kullanıcı en son aşamada şifresini girme işlemini bitirdiğinde yaptığı tıklamaları kontrol edebilir; hatası olduğunu fark ederse başa alıp tekrar tıklama işlemini yapabilir. Sistemin belirlediği tolerans değerleri içerisinde kullanıcının tıklamaları sistemde kayıtlı olan koordinatlar ile eşleştirilir. Tolerans değer içerisinde kalan tıklamalar geçerli olarak kabul edilir ve bütün tıklamalar geçerlilik sınırları içerisinde ise kullanıcının kimliği sistemde doğrulanır. Bu teknikte sisteme giriş işlemi uzun sürebilmektedir ve kullanıcıda bıkkınlık yaratabilmekte ve geçerli bir kullanıcı bile sistemde doğrulanamayabilmektedir.



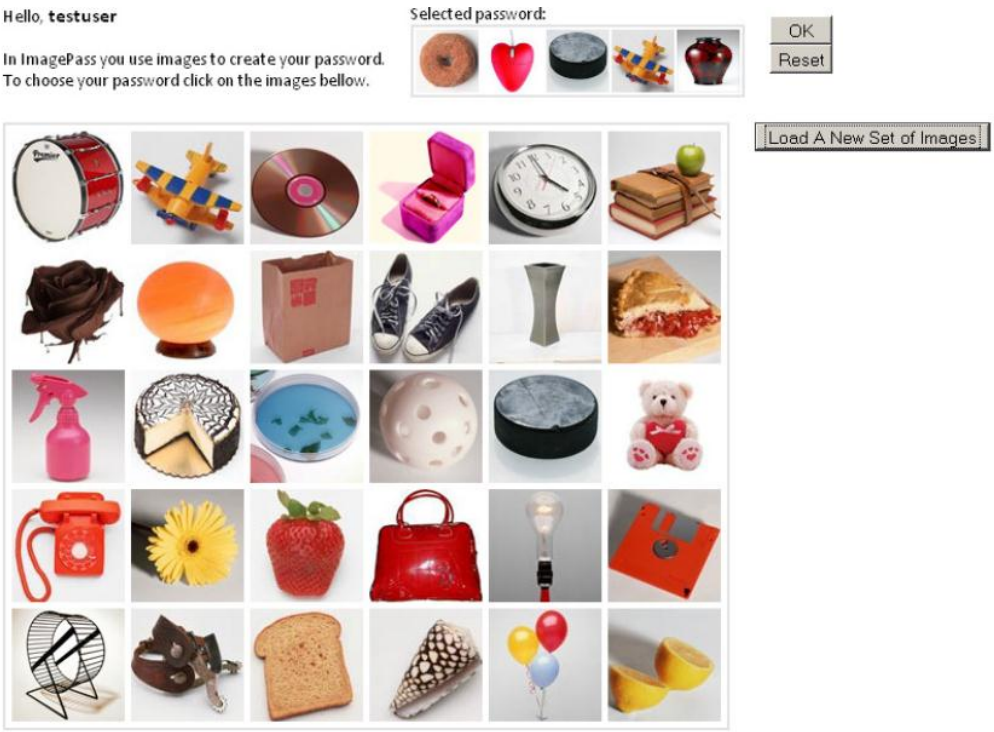
Şekil 2.14 Resim üzerinde istenen alanlara tıklama yöntemi kimlik doğrulama ekranı (Wiedenback vd. 2005)

Şifre uzayı da alfasayısal alfasayısal şifrelerde 64^8 ise bu yaklaşımda 1024x752'lik tam ekranın kullanıldığı varsayılsa ve her nokta 20x20 tolerans ile belirlenmiş olsa, sisteme de 5 tıklama ile girildiği varsayılsa şifre uzayı $(((1024x752)/(20x20)))^5$'den $(2.6x10)^{16}$dır. Bu teknikte üretilen şifre uzayı alfasayısal şifrelere göre oldukça büyüktür; fakat bu yaklaşım omuz sörfüne karşı dirençli değildir. Seçilen noktaları ekranı gören herhangi bir başka kullanıcı kaydedebilir.

2.2.11 Resim şifre yöntemi

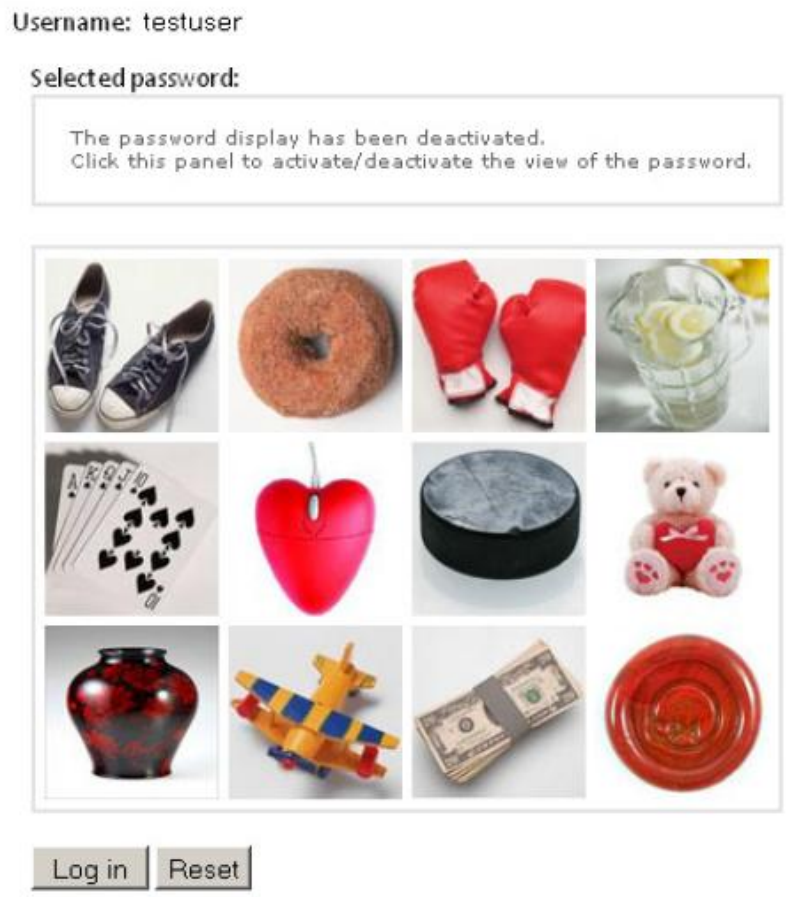
Resim şifre yöntemi Mihajlov (2011) tarafından geliştirilmiştir. Bu yöntemde kullanıcı şu şekilde sisteme kayıt olur: İlk aşamada kullanıcı adı belirlenir; sistemde tanımlı olmayan yeni bir kullanıcı adı belirlenene kadar ikinci aşamaya geçilmez. İkinci aşama görsel şifrenin belirleneceği kısımdır. Sistemin büyük bir resim veritabanı bulunmaktadır. Kullanıcıya bu veritabanından rastgele seçilmiş 30 adet resim içeren bir resim kümesi hücreler içinde sunulur (Şekil 2.15). Kullanıcı bu kümeyi beğenmezse yeni bir küme seçebilir ve yeni 30 resim içeren kümeden seçimlerini yapabilir. Her resim 90x90 piksel boyutlarındadır. Sistem tasarlanırken tüm resimler bazı kriterlere

göre seçilmiştir: her resim; bir nesne ile aydınlık bir arkaplandan oluşmaktadır. Sisteme girerken kullanıcı n sayıda seçim yapar; seçtikleri yukarıda seçilen şifre panosuna (selected password panel) sırayla yerleştirilir (Şekil 2.15).



Şekil 2.15 Resim şifre yöntemi şifre oluşturma ekranı (Mihajlov 2011)

Kullanıcı seçtiklerinden birini beğenmezse ya da birkaçını beğenmezse; üzerlerine tıklayıp bu resimleri kaldırabilir; hatta tamamiyle tüm seçtiği resimleri kaldırabilir ve sonrasında yeniden seçimler yapabilir. Kullanıcının oluşturabileceği şifre maksimum 7 boyutunda olabilir; kullanıcı 7'den daha kısa bir şifre de oluşturabilir örneğin 5'lik resim içeren bir şifre oluşturmuş olabilir. Arkada planda ise her zaman 12'lik şifre oluşturulmaktadır. Eğer kullanıcı kayıtta 5'lik bir şifre seçmişse; sistem 7 de kendi eklemektedir. Eklenen sahte resimler her oturumda aynıdır; aynı olmadığı durumda sistemi izleyen birisi tekrar etmeyen 7 adet resmi tespit edip kullanıcının oluşturduğu 5 uzunluğundaki şifreyi kırabilir. Kullanıcının şifresi bu değişmeyen 12'lik dizi olarak tutulur sistemde. Kullanıcı şifreyi oluşturduktan sonra bu kısmı tamamladığını belirtir. Sonrasında kullanıcıdan bir doğrulama istenir (Şekil 2.16). Doğrulama ekranı kullanıcının uygulamaya girme ekranının aynısıdır. Bu ekran her satırda 4 adet, her sütunda 3 adet olmak üzere toplam 12 adet resim içermektedir.



Şekil 2.16 Resim şifre yöntemi şifre doğrulama ekranı (Mihajlov 2011)

Uygulamaya girme ekranından farklı olarak sisteme kayıt sonrasında çıkan doğrulama ekranında bir kereliğine "Şifremi Göster" seçeneği kullanıcıya sunulur. Şifre girmeyi aktive etmek için ilgili kısma tıklanması gerekmektedir. Ekran ilk açıldığında 12lik resim kümesi yüklenir ve sisteme her girişte aynı resimler gelir; fakat her sisteme girişte resimlerin sırası değişir. Kulllanıcı doğru resimleri doğru sırada girince sisteme erişim hakkı kazanır. Kullanıcı birçok kez hatalı giriş yapabilir; fakat her 5 yanlış girişten sonra kimlik doğrulama işlemi değişir. Bu noktadan sonra sistem yöneticisi ile iletişime geçmelidir; sistem yöneticisi gelen kullanıcının sistemde geçerli bir kullanıcı olduğundan emin olduğunda kendisine yeni bir sisteme giriş anahtarı tanımlayacaktır.

Her resim şifre sisteminde farklı resim kümeleri kullanılması daha sağlıklı olacaktır yoksa kullanıcı her sistemde aynı resimleri seçebilir. Her kullanıcıya farklı bir resim

kümesi sunulursa şifrelerin de otomatikman farklı olması sağlanabilir; iki ayrı kullanıcının aynı şifreye sahip olması tercih edilmeyen bir durumdur.

Bu yöntemde şifre uzayının boyutu ise aynı resmin bir daha kullanılmasına izin verilmişse şifre uzunluğuna göre çizelge 2.3'teki gibidir.

Çizelge 2.3 Resim şifre yönteminde şifre uzayı karşılaştırılması

Şifre Uzunluğu	Kayıtta Oluşabilecek Minimum Şifre Uzayı Boyutu	Kimlik Doğrulamadaki Şifre Uzayı Boyutu
3	27000	1728
4	810000	20736
5	24300000	248832
6	729000000	2985984
7	21870000000	35831808

Bu sistemde kabakuvvet saldırılarına karşı güvenliği arttırmak adına bazı tedbirler alınmıştır. Bunlardan ilki kayıtta ve sisteme girerken kullanılan kullanıcı adı sistem içinde örneğin sistemin menüleri arasında geçiş yaparken farklı gösterilmektedir. Burada omuz sörfü ile kullanıcı adının görülmesine engel olmaktır. Diğer bir önlem de her bir resme eşsiz bir numara atamak ve tarayıcı üzerinden bu atanan numaralara denk gelecek şekilde başka numaralar yollamaktır. Örneğin elma için 1, armut için 2 olan eşsiz değerler tarayıcı üzerinden 1 değil 356, 2 değil 34 olarak yollanır. 356 olarak yollanan 1 değeri sistem içerisinde tekrar 1 olarak algılanacaktır. Üçüncü bir tedbir olarak da sistem; xhtml içinde resim adlarını rastgele bir anahtar ile hesaba dayalı adresleme (hashing) işlemine tabi tutulmaktadır. Sistem <img src="resimler\elma.jpg" id=1"> bilgisini <img src="images\ejxhy.jpg" id=356"> şeklinde tutmaktadır. Son bir tedbir olarak da 5 tane başarısız girişimden sonra saldırgan sıralı bir şekilde devam edemesin diye resimlerin sırası değiştirilmektedir. Bu durumda saldırgan nerede kaldığını tespit edemez (Mihajlov 2011).

2.2.12 Melez Grafiksel Kimlik Doğrulama Yöntemi

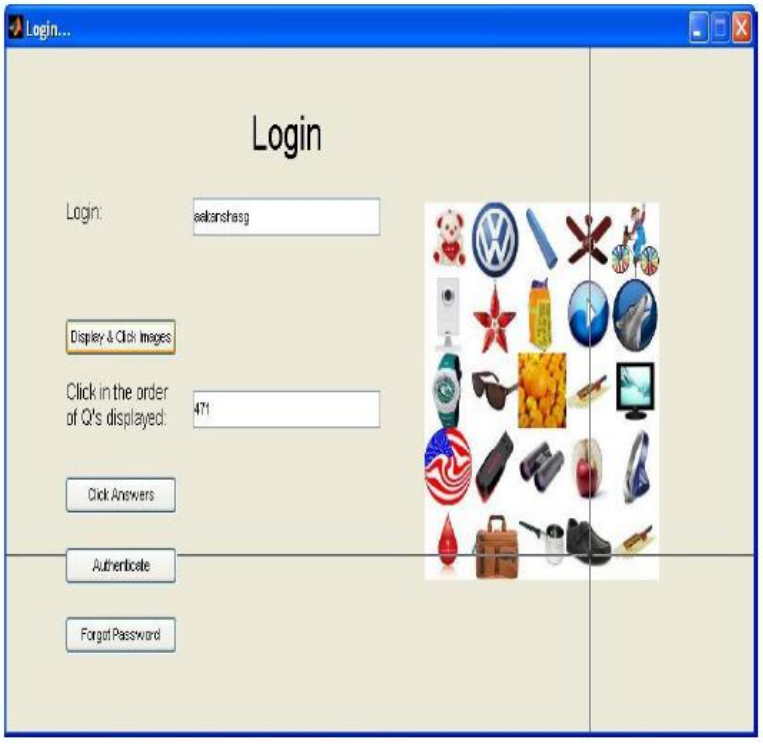
Tanıma tabanlı ve anımsama tabanlı görsel şifre tekniklerini içeren melez bir grafiksel kimlik doğrulama yöntemi geliştirilmiştir (Gokhale ve Waghmare 2014). Bu yöntemde kullanıcı kayıt olurken iki farklı şifre belirlemektedir. Kullanıcı birinci şifresini kendisine sunulan 25 adet resimden 6'sını seçerek oluşturmaktadır (Şekil 2.17).

Şekil 2.17 Kullanıcının sisteme kayıt olmasının ilk aşaması

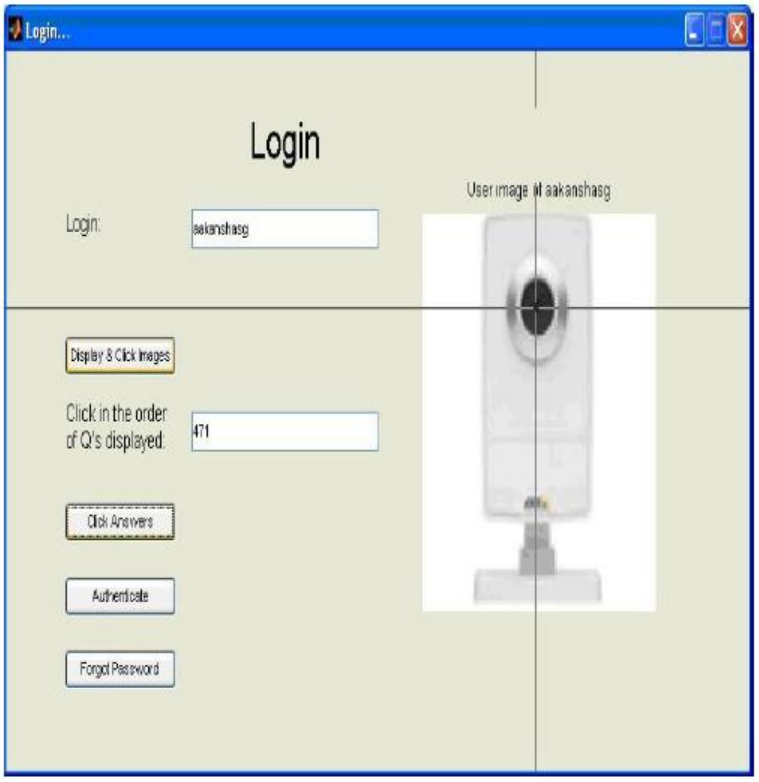
Bu resim kümesi tüm kullanıcılar için ortaktır. Kullanıcı ikinci şifresini ise sisteme kendi yüklediği bir resim üzerinde belirlenen sayıda alana tıklamak suretiyle oluşturur. Kullanıcı her bir alana karşılık gelen bir soru numarası seçer ve bu soruya cevap olarak bir alana tıklar (Şekil 2.18).

Şekil 2.18 Kullanıcının sisteme kayıt olmasının ikinci aşaması

Bu alanlar hayali bir kare ile tanımlanır ve her karenin x ve y koordinatlarında tolerans değerleri vardır. Diğer kişisel bilgiler de sisteme girildikten sonra kayıt işlemi tamamlanır. Kullanıcı sisteme giriş yapmak istediğinde öncelikle 25 resim arasından kendi şifresini oluşturan belirtilen sayıda resmi seçer (Şekil 2.19). Resim seçme aşaması tamamlandıktan sonra kullanıcıdan kayıt aşamasında seçtiği sorulara cevap olan alanları tıklaması istenir (Şekil 2.20). Her sisteme girişte sorular farklı sırada yöneltilebilmektedir. Kullanıcının sıraya uygun olarak ilgili alanlara tıklaması istenmektedir. Kullanıcı iki şifreyi de doğru girdiği takdirde kimliği sistemde doğrulanır. Bu yöntemde kimlik doğrulamanın ilk aşaması tanıma, ikinci aşaması ise anımsama tabanlıdır; ilk aşamada kullanıcı kendi şifresini oluşturan resimleri tanımaya çalışır, ikinci aşamada ise kayıtta oluşturduğu şifresini tekrar oluşturmaya çalışır.



Şekil 2.19 Tanıma tabanlı kimlik doğrulama aşaması



Şekil 2.20 Anımsama tabanlı kimlik doğrulama aşaması

Bu yaklaşımın ilk aşamasının şifre uzayı; p maksimum seçilebilecek resim sayısı olursa:

$$R_1 = \sum_{i=1}^{p} 25^i$$

olarak hesaplanır. Yöntemin ikinci aşamasının şifre uzayı ise; MxN resim portfolyosunun boyutları, q seçilebilecek maksimum soru sayısı, n^2 her soru için tıklanabilecek alan olursa:

$$R_2 = \sum_{j=1}^{q} \left(j! \times \left[\frac{M \times N}{n^2}\right]^j \right)$$

olarak hesaplanır. İki aşamanın şifre uzayları birleştirilirse tüm yaklaşımın şifre uzayı:

$$P = R_1 \times R_2$$

olarak hesaplanır. Yöntem büyük bir şifre uzayına sahip olma yeteneğindedir. İki aşamalı olması da sistemde oluşturulan şifrelerin kırılmasını güçleştirmektedir. İkinci safhada kullanıcının resmi sisteme yüklemesi de sistemin başka bir artısıdır. Belli tolerans değerleri içerisindeki alanlara tıklama durumu yanlış negatiflerin sayısının artmasına neden olabilir. Geçerli bir kullanıcı; +5,-5'lik tolerans değerleri içerisindeki alanı 1 piksel değeriyle kaçırırdığında kimliği sistemde doğrulanamayacaktır. Sistemde tolerans değerleri de iyi ayarlanmalıdır; yüksek tolerans değerleri yanlış pozitiflerin, düşük tolerans değerleri de yanlış negatiflerin çoğalmalmasına neden olabilmektedir.

Yöntem omuz sörfüne karşı dirençli olarak değerlendirilebilir; çünkü ikinci aşamada kullanıcının hangi alana tıkladığını anlamak sisteme girişi izleyen biri tarafından anlaşılamaz. Bu kimlik doğrulama yönteminin de diğer kimlik doğrulama yöntemleri gibi ödünleşimleri vardır. Tıklanan bölgelerin herhangi bir çerçeve içine alınmamış olması omuz sörfü açısından olumlu bir özellik olmasına rağmen kullanıcı açısından eksi bir özelliktir; çünkü kullanıcı nereye ne kadar tıkladığını nerede kaldığını bilememektedir.

3. KURAMSAL TEMELLER

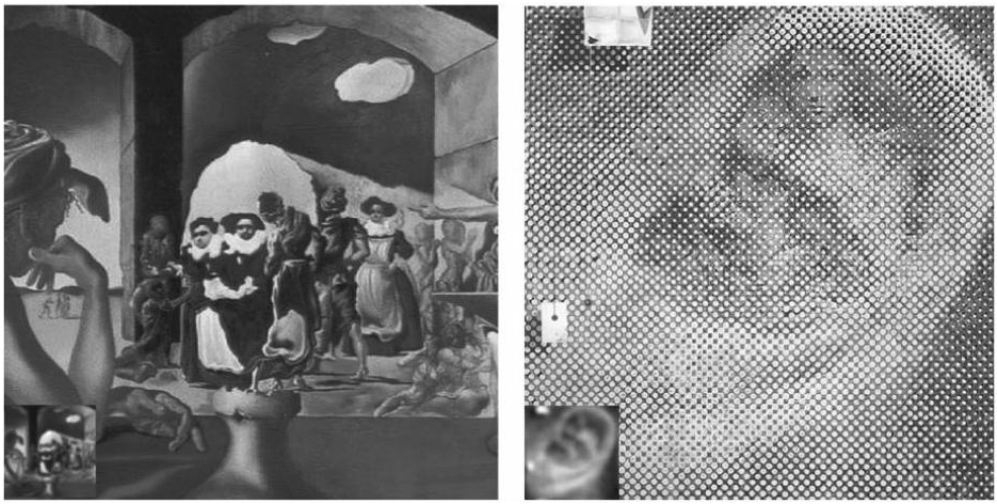
Bu tez kapsamında öngörülen grafik tabanlı kimlik doğrulama yönteminde mevcut kimlik doğrulama yöntemlerinden farklı olarak hibrit resimler kullanılmaktadır. Önerilen yönteme geçmeden önce hibrit resimler ile ilgili teoriksel bir altyapı sunmak faydalı olacaktır. Hibrit resim bir resmin düşük uzaysal frekansları ile başka bir resmin yüksek uzaysal frekanslarının kombinasyonu sonucu üretilen başka bir resimdir (Olive vd. 2006). Şekil 3.1-3.2'de birer hibrit resim örneği verilmektedir. Bu iki resim aslında aynıdır; fakat resme yakından bakıldığında bir evin tadilat görmekte olan hali görünmektedir (Şekil 3.1). Uzak mesafeden bakıldığında ise aynı evin tadilatı bitmiş hali görünmektedir (Şekil 3.2).

Şekil 3.1 Yakın mesafeden evin görünüşü (Oliva vd. 2006)

Şekil 3.2 Uzak mesafeden evin görünüşü (Oliva vd. 2006)

Hibrit resimlerin bu şekilde yorumlanmasını sağlayan insanın görme sisteminin çok ölçekli resim işleyebilme mekanizmasıdır (Oliva vd. 2006). Algısal gruplama mekanizmaları dikkate alınarak iki farklı yorumu olan hibrit resimler elde edilebilir.

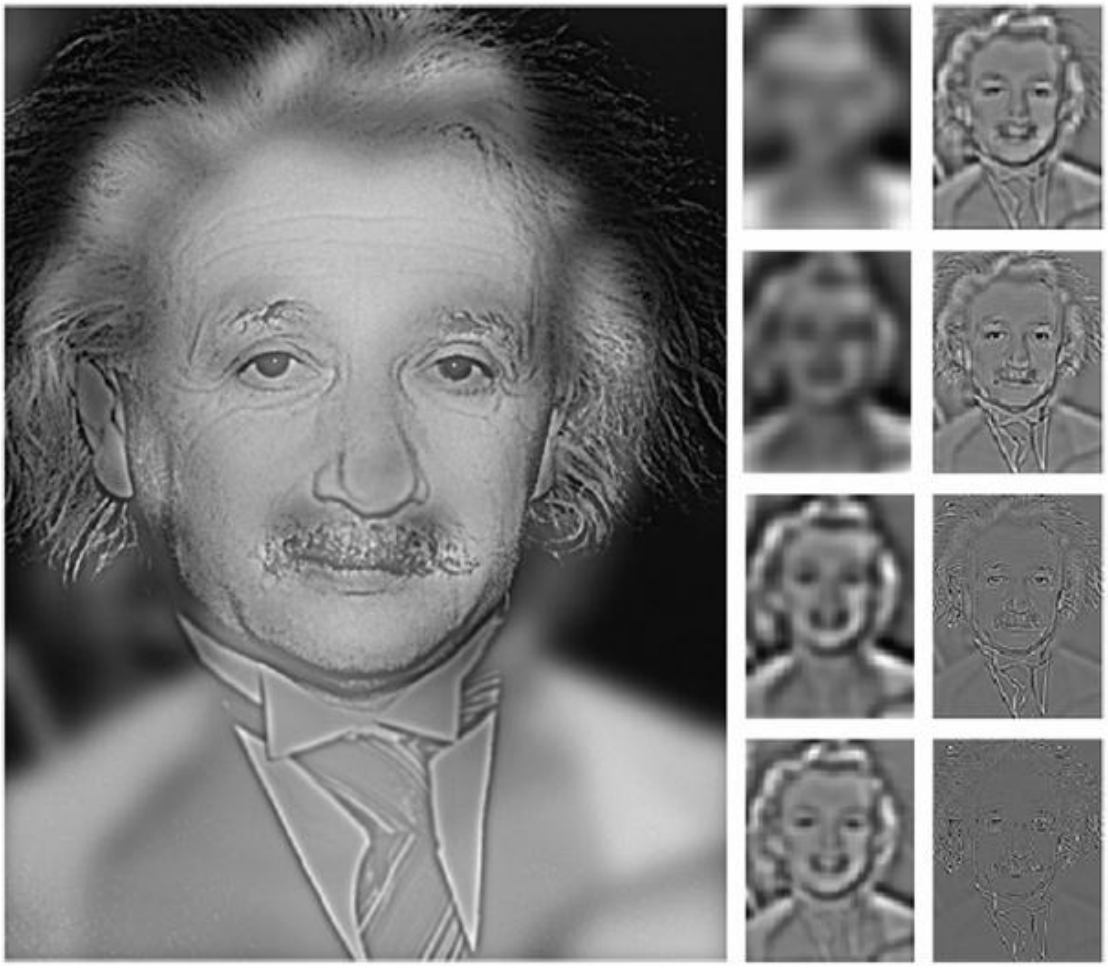
Günümüze kadar birçok sanatçı, tasarımcı, görsel bilim insanı bir resimden birçok anlam çıkarılmasını sağlamanın yollarını aramışlardır. Örneğin Salvador Dali'nin iki eserinde aynen hibrit resimlerdeki gibi resmin farklı boyutlarında farklı yorumlar yapmak mümkündür. Şekil 3.3.a'da resim küçültüldüğünde Voltaire'in büstü, büyütüldüğünde ise köle pazarı görünmektedir. Şekil 3.3.b'deki Madonna eserinde ise resmin küçük halinde bir kulak görünmekteyken, resmin büyük halinde ise bayan Madonna ve bir çocuk görünmektedir (Oliva 2013). Resimlere bakıldığında ortaya çıkan iki farklı algının insanın görsel sisteminin farklı bölgelerinin devreye girmesi sebebiyle olduğu öne sürülmüştür. (Gosselin ve Schyns 2001, Bonnar vd. 2002) Aynı çalışmalarda bu farklı bölgelerde yerel uzaysal filtrelerin olduğu öne sürülmüştür.



Şekil 3.3.a. Kaybolan Voltaire büstü ve köle pazarı, b. Madonna (Oliva 2013)

Her resim farklı uzaysal frekanslarda bileşenlerden oluşur. Bir resmin düşük uzaysal frekansları resmin bulanık, kararsız, keskin olmayan kontürlere sahip bölümleridir. Aynı resmin yüksek uzaysal frekansları ise keskin geçişleri olan, detayların daha net görüldüğü bölümleridir. Şekil 3.4'te Albert Einstein'ın resminin yüksek frekansları ile Marilyn Monroe'nun resminin düşük frekanslarının birbirine eklenmesi sonucu elde

edilen bir hibrit resim örneği verilmiştir. Resme yakından bakıldığında Einstein, uzaktan bakıldığında ise Monroe görünmektedir. Hibrit resmin yan kısmında bulunan küçük resimlerden düşük frekanslarda olanlarında sadece Marilyn Monroe görünmektedir ve hiçbir detay gözlenememektedir.



Şekil 3.4 Değişik frekanslardaki Marilyn Monroe ve Albert Einstein (Oliva 2013)

Bu resimlerde genel olarak Marilyn'in kafasının şekli ve büstü anlaşılmaktadır; frekans arttıkça gözleri, ağzı, burnu ve saçları seçilebilmektedir. Bir resme uzaktan bakıldığında düşük frekanslar gözlemlenebilir; örneğin bir kişinin yüzüne 10 metre uzaktan bakıldığında yüzünün bir bayana mı bir erkeğe mi ait olduğuna dair yorum yapılabilir; fakat yüzündeki ifadeye ya da yaşına dair bir yorum yapmak güçtür (Sowden ve Schyns 2006, Brady ve Oliva 2012) Yine şekil 3.4'te bulunan küçük resimlerden yüksek frekanslarda olanlarda ise en keskin ve en küçük detaylarına kadar Einstein'in sakalı,

kravatı gözlemlenebilmektedir. Bu yüksek frekanslı resimlerde Marilyn tamamen yokolmuştur. Bu örnekten yola çıkarak, hibrit resimlerin bulanık bir resim ile keskin hatları olan bir resmin birbirleri üzerine eklenerek üretilebileceği sonucuna varılabilir. Şekil 3.4'te görüldüğü üzere hibrit resim elde etmek için Marilyn Monroe resmi düşük frekansları geçiren bir filtreden, Einstein resmi ise yüksek frekansları geçiren bir filtreden geçirilmiştir. Tek bir filtre kullanarak aynı sonucu elde etmek de mümkündür. Yüksek uzaysal frekansları geçiren bir filtreden geçirilmek istenen resmin; düşük uzaysal frekansları geçiren bir filtreden geçirilmesiyle elde edilen sonuç resmin kendisinden çıkarıldığında; yüksek uzaysal frekanslı resim elde edilebilir. Hibrit resimler formülize edilmek istendiğinde hibrit resim H; birinci resim I1, ikinci resim I2, F düşük frekansları geçiren bir filtre olmak üzere:

$$H = I1 \cdot F + I2 \cdot (1-F)$$

olarak bulunur. Bütün işlemler Fourier nüfuz sahasında (domain) tanımlanmıştır. Hibrit resimler iki parametre ile belirlenir: alçak çözünürlükte (uzaktan bakınca görünebilecek) olan resmin frekans kesmesi (frequency cut) ile yüksek çözünürlükte (yakından bakınca görülecek) olan resmin frekans kesmesi. Alçak frekansları geçiren filtre olarak da Gauss filtresi kullanılabilir.

İnsanın resim algısı çalışmaları çerçevesinde, hibrit resimler farklı frekans kanallarının karakterize edilmesini ve uzaysal frekansların algıda işlenmesinin zaman açısından yorumlanmasını sağlaması açısından önemli bir yer tutmaktadır. Hibrit resimler; uzaklık ile oynanarak resimlerin yorumlarının değişebilceği yeni bir paradigma sunmaktadır. Bu paradigmada; belli bir bakma mesafesinde, belli bir frekans aralığında belli bir uzaysal frekans insanın resim algısında daha baskındır (Oliva 2006 vd.).

Teorik olarak her iki resmin birleşiminden bir hibrit resim elde edilebilir; fakat estetik olarak istenen düzeyde hibrit resimler elde etmek için bazı kurallara uymak gerekmektedir. Eğer hibrit resimdeki iki resimden biri daha baskınsa, alternatif resmi görmek zorlaşacaktır. Resme bakılan mesafe değiştikçe anlamının da değişmesi gerekmektedir. Görülmesi beklenen resim rahatlıkla görülmeli, görünmesi istenmeyen

resim de gürültü olarak algılanmalı ya da görünmesi beklenen resim içinde kaybolmalıdır.

Görsel tabanlı şifrelerin en büyük problemi omuz sörfü olarak adledilmektedir (Anderson 1993). Yakından bakıldığında farklı, uzaktan bakıldığında farklı algılanmasından dolayı; bu tez çalışmasının fikir aşamasında hibrit resimlerin omuz sörfü problemine bir çözüm olabileceği düşünülmüştür. Bu tez çalışması kapsamında öngörülen grafik tabanlı kimlik doğrulama yöntemine omuz sörfüne dirençli olma özelliğini hibrit resimler vermektedir.

4. ÖNERİLEN KİMLİK DOĞRULAMA YÖNTEMİ

Bu tez çalışması kapsamında alternatif bir kimlik doğrulama yöntemi üzerinde durulmaktadır. Bu alternatif yöntem grafik tabanlıdır ve omuz sörfüne dirençli olacak şekilde kurgulanmıştır. Öngörülen yöntem hatırlama tabanlıdır. Anımsama tabanlı görsel kimlik doğrulama yöntemlerinin; hatırlama tabanlı yöntemlere göre kullanıcı deneyimi açısından daha zorlayıcı olduğu öne sürülmüştür (Tulving ve Watkins 1973). Bu tespite dayanak olarak da; anımsama tabanlı yöntemde kullanıcının kayıt olurken ürettiği bir şekli, resmi sıfırdan tekrar üretmesi; hatırlama tabanlıda ise böyle bir işlem yapmaması gösterilmiştir. Yine başka bir çalışmada da tanıma tabanlı görsel şifrelerin anımsama tabanlı görsel şifrelere göre iyi bir yöntem olduğu öne sürülmüştür (Norman 1988). Daha iyi bir yöntem olduğuna dayanak olarak da bellekte ikili bir bilgi tutulması gösterilmiştir. Kullanıcı bir resmi/görseli şifresinde ya kullanmıştır ya da kullanmamıştır, yeniden bir şifre üretmeyecektir ve hiçbir şekilde herhangi bir kelime ya da rakamı ezberlemesine gerek olmayacaktır. Öngörülen yöntemin; kullanım kolaylığı ve yanlış negatifleri minimuma çekmek esas olduğu için hatırlama tabanlı olmasına karar verilmiştir.

Öngörülen yöntemde kullanıcı sisteme kayıt olurken benzersiz kullanıcı adını belirledikten sonra 5x5'lik siyah beyaz bir resim kümesinden 6 adet resim seçer ve hemen akabinde seçtiği resimleri düşünerek bir hikaye üretir. Seçilen resimlerin daha iyi hatırlanabilmesine katkıda bulunacağı düşünülerek hikayecilikten yararlanılmıştır. Yapılan bir çalışmada; bir hikaye ile desteklendiğinde rastgele seçilen resimlerin hatırlanabilirliğinin arttığı öne sürülmüştür (Norman 1988). Bu durum da hesaba katılarak görsel şifre oluşturulurken kullanıcının seçtiği resimlerden bir hikaye yazması istenmiştir. Şifreyi meydana getiren resimler seçilirken; resimlerin somut nesneler ya da durumlar içermesine özen gösterilmiştir. Yapılan bir çalışmada insanın uzun soluklu belleğinde resmin kendisinin değil; resmin anlamlı bir yorumunun tutulduğu öne sürülmüştür (Mandler ve Ritchey 1977). İnsan yüzlerini kullanmak da bir seçim olabilirdi; çünkü beyinde sadece insan yüzlerini tanımadan sorumlu bir bölge olduğu araştırmalarda ortaya konmuştur (https://www.huffingtonpost.com 2012). Farklı bir araştırmada ise geçiş yüzü uygulamasının bir analizi yapılmıştır ve insanların

seçimlerinde bazı örüntüler yakalanmıştır ve bu bir güvenlik açığına sebep olabilir (Davis vd. 2004).

Önerilen yöntemde resimlerin seçilmesi ve sonrasında hikayenin oluşturulması ile kayıt işlemi tamamlanır. Kullanıcı aynı resmi 2 kere seçemez, şifre 6 farklı resim ile sistemde temsil edilir ve yöntem arka planda resimlerin hangi sırayla seçildiğini tutmaz. Bu sebeple şifre uzayı P(25,6) = 127,512,000 olabilecekken; sıra dikkate alınmadığı için C(25,6) = 177,100 olarak hesaplanır. Şifreyi temsil eden resimlerin kendileri değil; indeksleri veritabanına adrese dayalı hesaplama yöntemi (hashing) ile kaydedilir. Resmin kendisini direkt tutmak maliyetli olacağı için doğrudan indeksi tutmak sınırlı olan kaynakları daha verimli kullanmakta faydalı olmaktadır. Hikaye de en az 80 karakter olmalıdır ve boş girilemez. Hikaye kısmına yazılan metin arka planda tutulmaz. Hikayecilikteki tek amaç şifrenin daha iyi hatırlanmasını sağlamaktır.

Kayıtlı kullanıcı sisteme giriş yapılırken benzersiz kullanıcı adını klavyeden girdikten sonra 5x5'lik resim kümesinden sıra düşünmeksizin şifreyi oluşturan 6 resmi hatırlamaya çalışır ve kullanıcının kimliği sistemde doğrulanır ya da şifrenin yanlış olduğu belirtilerek tekrar girmesi istenir. Kullanıcı şifresini en fazla 3 kere yanlış girebilir. Kabakuvvet saldırısına karşı sistem kendini 3 kere yanlış girmeden sonrasına izin vermeyerek korur. Kullanıcı 25 adet resim içerisinden seçim yaparken seçtiği resimlerin etrafında bir çerçeve oluşturulur, bu çerçeve oluşturulmadığı zaman kullanıcılar hangi resmi seçtiklerinden emin olamayıp yanlış negatife düşebilirler ve kullanım zorluğu oluşabilir; bu istenen bir durum değildir.

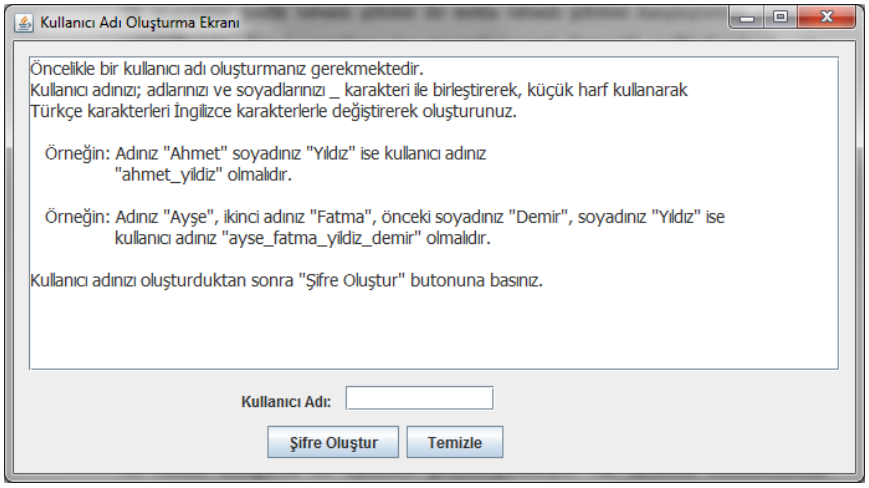
Önerilen yöntemde benzersiz kullanıcı adını girme kısmının dışında tüm işlemler fare tıklaması ile yapılmaktadır. Bu durum ajan yazılımların veya klavyeyi takip eden yazılımların şifreyi ele geçirmesine engel olmaktadır. Fare tıklamasıyla elde edilen veriler üzerinden de şifrenin ele geçirilmesi pek mümkün değildir. Bu verilerin tıklamayı yorumlayacak olan programın uygulama bilgisi, pencerenin konumu, boyutu ve zamanlama bilgisi ile birleştirilmesi gereklidir; ancak diğer bilgiler de elde edilirse bir yorum yapılabilir. Alfasayısal şifrelerdeki en büyük sıkıntılardan birisi de doğrudan klavyeden veri girilmesidir. Öngörülen yöntem bu açıdan daha güvenlidir.

Buraya kadar önerilen alternatif grafik tabanlı kimlik doğrulama yöntemi önceki çalışmalardan çok farklı değildir. Yöntemi benzerlerinden farklı kılabilecek olan; omuz sörfü problemine pratik bir çözüm getirmek istemesidir. Denkleme omuz sörfüne dirençli olma özelliğini eklemeden önce öngörülen yöntemi klasik alfasayısal tabanlı kimlik doğrulama ile karşılaştıran bir kullanıcı deneyimi araştırması yapılmıştır. Bu araştırma ile maksat yöntemin klasik alışılmış bir metin tabanlı kimlik doğrulama yöntemine hatırlanabilirlik, kullanılabilirlik açısından yaklaştığından emin olmaktır. Bu araştırma; öngörülen yöntemin de ötesinde metin tabanlı kimlik doğrulama ile genel grafik tabanlı kimlik doğrulama yöntemlerinin bir karşılaştırması olarak düşünülebilir ve elde edilen bulgular iki yöntemi karşılaştıran araştırmalarda kullanılabilir. Omuz sörfüne dirençli olma özelliği devreye girdiğinde resimler siyah beyaz olarak kullanıcıya sunulacaktır, çünkü renk parametresi devreye girerse gruplama işlemi kolaylaşır, yakından ve uzaktan görülen resimler daha net ayırt edilebilir (Oliva 2006). Renk değişkeninin hibrit resimlerin başarısını negatif etkileyebileceği düşünülerek tüm resimler grinin tonları (grayscale) olarak hibritlenecektir, uygulamada homojen bir yapı oluşması açısından omuz sörfüne dirençsiz kısımda da grinin tonlarını içeren resimler kullanılmıştır.

4.1 Metin Tabanlı Kimlik Doğrulama ile Alternatif Yöntemin Karşılaştırılması

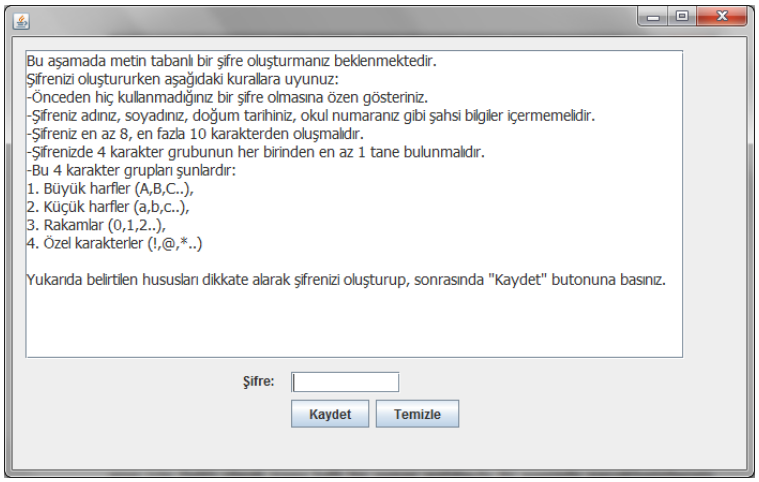
4.1.1 Alfasayısal ve grafik tabanlı şifrelerin oluşturulması

Grafik tabanlı şifreler ile alfasayısal şifreleri kullanıcı deneyimi açısından karşılaştırmak amacıyla bir uygulama geliştirilmiştir. Bilgisayar kullanma konusunda rahat olan, klavye ve fare kullanımı konusunda oldukça deneyimli 20 kullanıcı belirlenmiştir ve kullanıcılar uygulamadaki yönergeleri izleyerek tez çalışmasına katkıda bulunmuşlardır. Uygulamanın ilk aşamasında kullanıcılar; adlarını ve soyadlarını kullanarak eşsiz bir kullanıcı adı belirlemişlerdir (Şekil 4.1).



Şekil 4.1 Eşsiz kullanıcı adının belirlenmesi

Uygulamanın ikinci aşamasında; kullanıcılardan daha önce herhangi bir uygulamada kullanmadıkları, en az 8 en fazla 10 karakterlik, şahsi bilgiler içermeyen ve listelenen 4 karakter grubundan en az 1 tanesini içerecek şekilde bir şifre belirlemeleri istenmiştir (Şekil 4.2).



Şekil 4.2 Listelenen kriterlere uygun alfasayısal şifrenin oluşturulması

Uygulamanın üçüncü aşamasında ise kullanıcılardan 5x5'lik resim portföyünden 6 adet seçim yapmaları istenmiştir. Seçtikleri 6 resim kullanıcıların görsel şifrelerini oluşturmuştur (Şekil 4.3).

Şekil 4.3 Grafik tabanlı şifre oluşturma ekranı

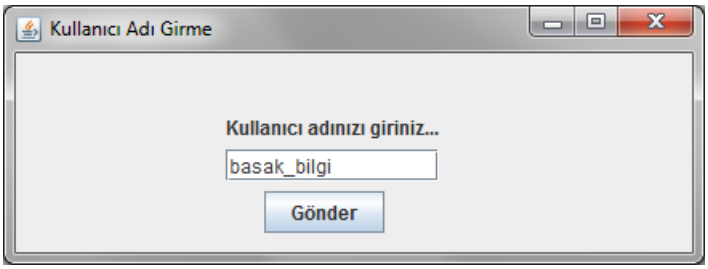
Uygulamanın dördüncü ve son aşamasında kullanıcılardan; oluşturdukları grafik tabanlı şifrelerinde bulunan resimlere bakarak bir hikaye yazmaları istenmiştir (Şekil 4.4).

Şekil 4.4 Görsel tabanlı şifreyi kullanarak hikaye oluşturma ekranı

Hikayelerini tamamladıktan sonra kullanıcıların sisteme kayıt işlemi tamamlanmıştır. Grafik tabanlı şifreler arka planda resim indeksleri ile sistemde temsil edilmiştir. Belirlenen alfasayısal ve grafik tabanlı şifreler kullanıcı adıyla birlikte hesaba dayalı adresleme işleminden geçirilerek veri tabanına kaydedilmiştir. Bahsi geçen tüm aşamaları tamamlayarak 20 kişinin sisteme kayıt olması sağlanmıştır.

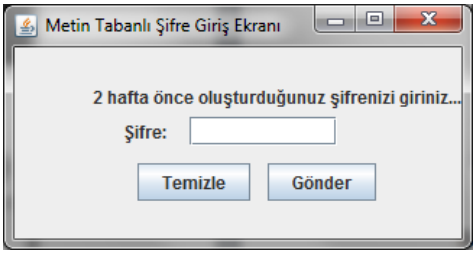
4.1.2 Oluşturulan şifreleri kullanarak sisteme giriş

Sisteme kayıt olan 20 kişiden aralıklarla şifrelerini 3 kez girmeleri istenmiştir. Birinci sisteme giriş; sisteme kayıt olmanın hemen akabinde gerçekleşmiştir. İkinci sisteme giriş bir hafta sonra, üçüncü ve son sisteme giriş ise iki hafta sonra gerçekleşmiştir. Sisteme giriş ise üç aşamadan oluşmaktadır. Şekil 4.5'de görüldüğü üzere ilk aşamada kullanıcı eşsiz kullanıcı adını girer.

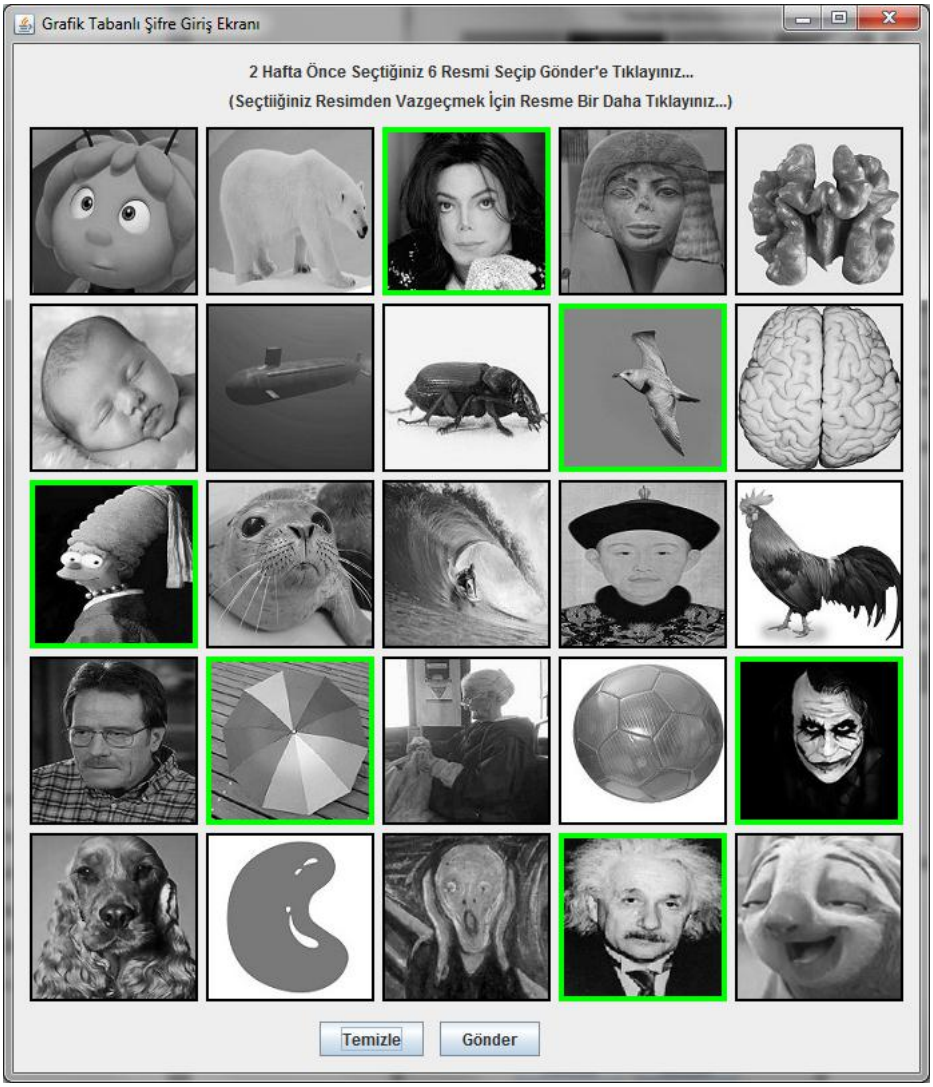


Şekil 4.5 Kullanıcı adı girme ekranı

İkinci aşamada kullanıcı daha önceden oluşturduğu alfasayısal şifresini girer (Şekil 4.6). Üçüncü ve son aşamada kullanıcı daha önceden seçtiği resimleri sırayı dikkate almaksızın hatırlamaya çalışıp tekrar seçmeye çalışır (Şekil 4.7).



Şekil 4.6 Alfasayısal şifre giriş ekranı



Şekil 4.7 Grafik tabanlı şifre giriş ekranı

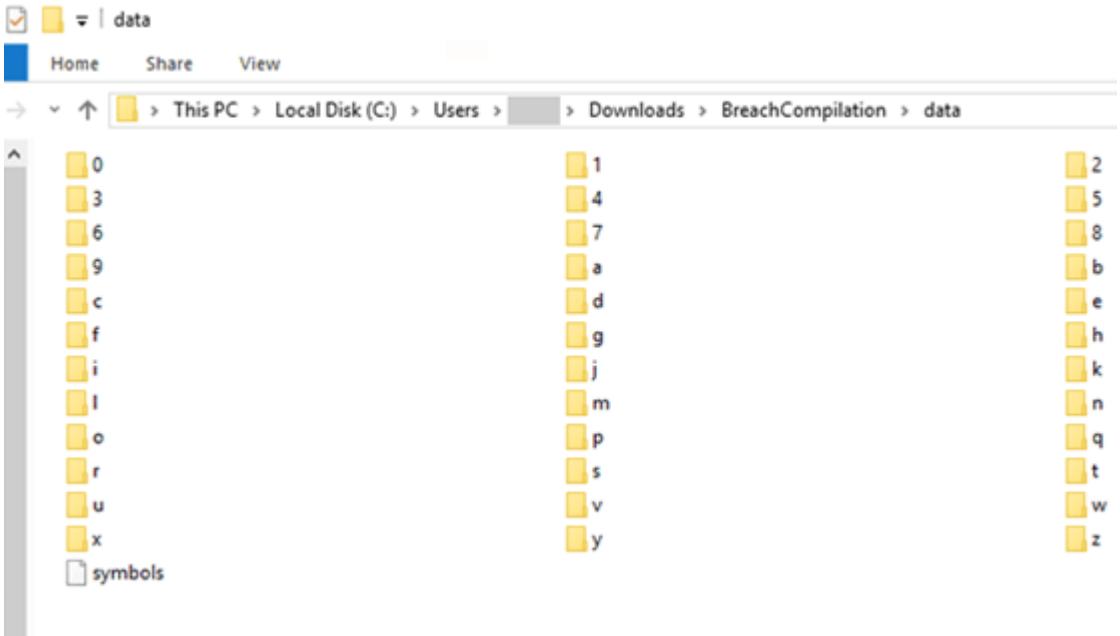
Şekil 4.6-4.7'de "2 hafta önce" ifadesi geçmektedir. Bu ifade; şifre oluşturmanın hemen akabindeki sisteme girişte "az önce" şeklinde, bir hafta sonraki sisteme girişte ise "bir hafta önce" şeklinde yer almıştır. Kullanıcılar toplamda üç kere şifrelerini girmek suretiyle iki haftalık çalışmayı tamamlamışlardır.

4.1.3 Elde edilen sonuçlar ve analiz

Alfasayısal kimlik doğrulama yönteminde kullanıcılardan en az 8, en fazla 10 uzunluğunda ve aşağıda belirtilen gruplardan her birinden en az 1 karakter içerecek şekilde şifrelerini oluşturmaları istenmiştir:

1. Büyük harfler (A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,V,Z)
2. Küçük harfler (a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,v,z),
3. Rakamlar (0,1,2,3,4,5,6,7,8,9),
4. Özel karakterler (!$%^&*()_-+=@#<,>.?,vb.)

Bu koşullar altında teorik olarak oldukça büyük bir şifre uzayı (94^N) oluşmaktadır; fakat daha önce de belirtildiği gibi şifre uzayı pratikte çok daha küçüktür (Bagchi ve Atluri 2006). Yakın zamanda 1.4 milyon adet şifre ve kullanıcı adı, elektronik posta kombinasyonu 41 GB boyutunda bir arşiv internet üzerinde dolandığına dair bir haber çıkmıştır (Anonymous 2017). Şekil 4.8'de görüldüğü üzere bu şifreler düzgün bir şekilde bölümlendirilmiş ve iki üç seviye olarak sıralanmıştır.



Şekil 4.8 Dev şifre arşivi (http://hackernews.com 2017)

Bu dev arşivin Bitcoin, Pastebin, LinkedIn, MySpace, Netflix, Last.FM, Zoosk, Badoo, RedBox, Minecraft and Runescape gibi uygulamalardan ya da diğer internet sitelerinden sızdırıldığı söylenmektedir. Bilgisayar korsanları bir kullanıcının şifresini ele geçirmeye çalıştıklarında ilk aşamada bu dev arşivde arama yapmaktalar (Anonymous 2017). Sitede en çok kullanılan şifreler de yayınlanmıştır. Şekil 4.9'da görüldüğü üzere "123456", "123456789", "qwerty," "password" ve "111111" en çok kullanılan şifrelerdir. Bu bilgilerin bilgisayar korsanlarının eline geçmesinin iki sebebi vardır: birincisi kullanıcılar her uygulamada aynı şifreyi kullanmaktadırlar, ikincisi de kullanıcılar çok basit şifreler seçmektedirler. Bu tez çalışması kapsamında oluşturulan alfasayısal şifrelerin bu iki güvenlik açığına sahip olmamasına özen gösterilmiştir. Kullanıcılar başka bir yerde kullandıkları şifreyi kullanmama noktasında özen gösterdiklerini belirtmişlerdir; fakat bu tam doğruluğundan emin olabilecek bir husus değildir. Oluşturdukları şifrelerin; araştırmayı yapan kişide düz metin olarak bulunmayacağı bilgisi kendileriyle paylaşılmıştır. Şifreler araştırmacıda da bulunmayacaktır; çünkü veritabanına şifrelerin kendisi değil hesaba dayalı adresleme (hashing) işleminden geçirilmiş şekilleri yazılmıştır. Şifreler sisteme girildiğinde girilen şifrenin özet değeri ile veritabanındaki özet değeri karşılaştırılacaktır. Hesaba dayalı adresleme yönteminde tersden gidip şifreyi elde etmek mümkün değildir. Aynı sitede

	Count	Password		Count	Password
1	9218720	123456	21	370652	666666
2	3103503	123456789	22	354784	123
3	1651385	qwerty	23	347187	monkey
4	1313464	password	24	343864	dragon
5	1273179	111111	25	311371	1qaz2wsx
6	1126222	12345678	26	300279	123qwe
7	1085144	abc123	27	299984	121212
8	969909	1234567	28	298938	myspac
9	952446	password1	29	291132	a123456
10	879924	1234567890	30	276473	qwe123
11	866640	123123	31	270488	1q2w3e4r
12	834468	12345	32	268121	zxcvbnm
13	621078	homelesspa	33	263605	7777777
14	564344	iloveyou	34	255079	123abc
15	527158	1q2w3e4r5t	35	250732	qwerty123

Şekil 4.9 Arşivde en çok kullanılan şifreler (http://hackernews.com 2017)

basit şifrelere karşılık "güçlü şifreler" seçilmesi gerektiği belirtilmektedir ve bazı güçlü şifre oluşturma yazılımlarına bağlantı verilmektedir. Yukarıda bahsedilen karakter grubundan her birini içeren şifreler "güçlü şifreler" olarak literatürde geçmektedir. Bu tez çalışmasında da "güçlü şifreler" oluşturulması zorunlu kılınmıştır. Beklendiği üzere kullanıcılar alfasayısal şifre oluşturma kısmında fazla zorluk çekmemiştir; fakat resimlerden seçim yapıp sonrasında seçilen resimleri dikkate alarak bir hikaye oluşturma kısmında biraz yabancılık yaşamışlardır; fakat genel olarak hemen adapte olmuşlardır. Grafik tabanlı şifre oluşturmada 25 resimden 6 resim seçilmesi istenmiştir ve tekrara izin verilmemiştir; dolayısıyla teoride C(25,6) boyutunda bir şifre uzayı oluşmuştur. Pratikte de bu şifre uzayının daha küçük olması için bir neden bulunmamaktadır. Grafik tabanlı şifreler basit şifre ya da güçlü şifre gibi de sınıflandırılamamaktadır; çünkü bir kombinasyonun başka bir kombinasyondan daha çok seçilmesi için bir sebep bulunmamaktadır. Resimler tamamen rastgele seçilmiştir. Şifreyi oluşturma aşamasında kullanıcılar istenen özelliklerde şifre oluşturana kadar denemelerine devam etmişlerdir. Şifrelerin kaç denemeden sonra oluşturulduğu bilgisi çizelge 4.1'de gösterilmiştir.

Çizelge 4.1 Şifrelerin kaç denemede oluşturulduğu

Kullanıcı	Metin Tabanlı Şifrenin Kaç Denemede Oluşturulduğu	Grafik Tabanlı Şifrenin Kaç Denemede Oluşturulduğu
1	2	1
2	2	2
3	3	1
4	1	1
5	2	2
6	2	1
7	2	1
8	2	2
9	3	1
10	4	2
11	2	1
12	2	2
13	4	1
14	3	1
15	2	1
16	1	2
17	1	1
18	3	2
19	2	1
20	2	2

Şifrelerin ne kadar sürede üretildiği bilgisi de çizelge 4.2'de gösterilmektedir.

Çizelge 4.2 Şifrelerin oluşturulma süresi

Kullanıcı	Metin Tabanlı Şifreyi Oluşturma Süresi (sn)	Grafik Tabanlı Şifreyi Oluşturma Süresi (sn)
1	85	61
2	115	65
3	99	74
4	104	61
5	113	48
6	103	62
7	91	56
8	87	58
9	114	69
10	113	75
11	47	62
12	67	71
13	111	78
14	46	72
15	82	65
16	101	61
17	122	47
18	102	57
19	79	66
20	76	64

Daha özet değerler elde edilmek istendiğinde çizelge 4.3'deki veriler elde edilmektedir.

Çizelge 4.3 Şifre oluşturma aşamasındaki deneme sayısı ve şifreyi oluşturma süresi

	Ortalama Deneme Sayısı	Ortalama Oluşturma Süresi (Standart Sapma)
Metin Tabanlı	2.25 (0.809)	92.85 (20.704)
Grafik Tabanlı	1.4 (0.478)	63.6 (7.827)

Grafik tabanlı şifreyi oluşturulurken geçirilen süre hesaplanırken hikaye yazma kısmı hesaba katılmamıştır; çünkü bu kısıma gelindiğinde şifre çoktan oluşmuştur; bu bölümü koymanın amacı hikaye yazarken kullanıcının resimleri aklına daha iyi yazmasını sağlamaktır.

Elde edilen verileri analiz etmek için T-testi yöntemi kullanılmıştır. İlk analiz şifrenin kaç denemeden sonra üretildiği üzerinde şifre yönteminin önemi olup olmadığına dairdir. T-testinde p değeri 0.001 olarak hesaplanmıştır. Bu değer p değerinin 0.005 sınır değerinden oldukça küçüktür. T-testine göre p değeri 0.005'ten küçük bulunursa test edilen durumların hangi sınıfa girdiğinin test sonucu üzerinde etkisi olduğu sonucuna varılır. Bu durumda alfasayısal şifre oluştururken yapılan deneme sayısı ile grafik tabanlı şifre oluşturulurken yapılan deneme sayısı arasında önemli farklar olduğu sonucuna varılır. Genel bir sonuca varılmak istenirse; "grafik tabanlı şifreler alfasayısal şifrelere göre daha az denemede oluşturulmuştur" denebilir. Aynı analiz şifre oluşturma süresi üzerinde yapıldığında p değeri 0.0000443429 olarak bulunmuştur. Bu değer 0.005 değerinden oldukça küçüktür; yorumu ise alfasayısal ya da grafik tabanlı olmanın şifre türünün üretilme süresinde çok büyük öneme sahip olduğudur. Yine genel bir sonuca varılmak istenirse; "grafik tabanlı şifreler alfasayısal şifrelere göre daha kısa sürede üretilmiştir" denebilir.

Sisteme ilk giriş şifrelerin oluşturulmasının hemen ardından olmuştur ve özet değerler çizelge 4.4'teki gibidir.

Çizelge 4.4 Sisteme şifreyi giriş sayısı ve geçen süre (şifreleri oluşturduktan hemen sonra

	Ortalama Deneme Sayısı	Ortalama Giriş Süresi (Standart Sapma)
Metin Tabanlı	1.6 (0.569)	64.35 (15.920)
Grafik Tabanlı	1.55 (0.575)	63.6 (7.827)

Elde edilen değerler üzerinden T-testi yapıldığında p değeri; deneme sayısı için 0.789, oluşturma süresi için 0.856 olarak hesaplanmıştır. Bu değerlerden çıkan sonuç; şifreler oluşturulduktan hemen sonra sisteme girildiğinde şifre tipinin herhangi bir önem arz etmediğidir.

Şifrelerin sisteme ikinci kez girilmelerinde ise çizelge 4.5'teki özet değerler elde edilmiştir. T-testi bir hafta sonraki veriler üzerinde uygulandığında p değeri; deneme sayısı için 0.0000213623, oluşturma süresi için de 0.00000689229 olarak

hesaplanmıştır. Bu değerlerden çıkan sonuç bir hafta sonrasında şifre tipinin deneme sayısı ve süresi üzerinde önemli olduğudur.

Çizelge 4.5 Sisteme şifreyi giriş sayısı ve geçen süre (1 hafta sonra)

	Ortalama Deneme Sayısı	Ortalama Giriş Süresi (Standart Sapma)
Metin Tabanlı	2.7 (0.543)	94.35 (15.920)
Grafik Tabanlı	1.75 (0.422)	67.85 (7.408)

Üçüncü ve son şifre girişlerinde elde edilen özet değerler çizelge 4.6'daki gibidir. T-testi iki hafta sonunda elde edilen veriler üzerinde uygulandığında da bir hafta öncekine benzer değerler elde edilmiştir. Aynı şekilde elde edilen p değerleri de yakındır. p değeri deneme sayısı için 0.00000414287, oluşturma süresi için de 0.0000105108 olarak hesaplanmıştır. Buradan çıkan sonuç iki hafta sonraki girişlerde de şifre tipi önem arz etmektedir.

Çizelge 4.6 Sisteme şifreyi giriş sayısı ve geçen süre (2 hafta sonra)

	Ortalama Deneme Sayısı	Ortalama Giriş Süresi (Standart Sapma)
Metin Tabanlı	2.90 (0.683)	95.35 (16.151)
Grafik Tabanlı	1.85 (0.348)	68.85 (8.195)

Bazı kullanıcılar ilk seferde şifreyi doğru girebilmiştir; bazıları ise 3 denemeden sonra bile şifresini doğru girememiştir; bu kullanıcılar için "Şifremi Göster" özelliği eklenmiştir. Şifrelerini gördükten sonraki girişler 4 denemede başarılı olmuş sayılarak verilere eklenmiştir.

Şifreleri sisteme giriş sisteme kaydın hemen sonrası, bir hafta sonrası ve iki hafta sonrası için olmak üzere üç ayrı zamanda gerçekleşmiştir. Bir analiz de zaman üzerinden yapılabilir. Çizelge 4.7'de alfasayısal şifrelerin birinci ve ikinci ile ikinci ve

üçüncü haftaların T-testine göre hesaplanmış p değerleri bulunmaktadır. Rakamlar üzerinden bir analiz yapmak istenirse; birinci ve ikinci şifreye girişte yapılan deneme sayıları ile giriş süreleri arasında ciddi bir fark olduğu sonucuna varılır. İkinci ve üçüncü haftalardaki girişlerde böyle bir fark bulunmamıştır. Kullanıcılar; şifrelerini ikinci girişlerinde ne kadar hatırlamışlarsa benzer seviyede üçüncü girişlerinde de hatırlamışlardır.

Çizelge 4.7 Alfasayısal şifre için her hafta ikilisi için hesaplanan p değerleri

	Birinci Hafta ile İkinci Haftanın p Değeri	İkinci ve Üçüncü Haftanın p Değeri
Kaç Denemede Doğru Girildiği	<0.05	0,0420863
Geçen Süre	<0.05	0,1036032

Çizelge 4.8'de ise grafik tabanlı şifrelerin birinci ve ikinci ile ikinci ve üçüncü haftaların T-testine göre hesaplanmış p değerleri bulunmaktadır. Rakamlar üzerinden bir analiz yapmak istenirse; birinci ve ikinci şifreye girişte yapılan deneme sayıları ile giriş süreleri arasında ciddi bir fark olmadığı sonucuna varılır. İkinci ve üçüncü haftalardaki girişlerde de böyle bir fark bulunmamıştır. Kullanıcılar; şifrelerini ilk girişlerinde ne kadar hatırlamışlarsa benzer seviyede ikinci ve üçüncü girişlerinde de hatırlamışlardır.

Çizelge 4.8 Grafik tabanlı şifre için her hafta ikilisi için hesaplanan p değerleri

	Birinci Hafta ile İkinci Haftanın p Değeri	İkinci ve Üçüncü Haftanın p Değeri
Kaç Denemede Doğru Girildiği	0,103603159	0,32988
Geçen Süre	0,00997	0,27902

Resimlerin sırasının ezberlenmesi kullanım kolaylığını azaltmakta ve yanlış negatiflerin sayısının artmasına neden olmaktadır. Metin tabanlı şifreler ile grafik tabanlı şifreleri kullanıcı deneyimi açısından değerlendirmek amacıyla geliştirilen uygulamada bazı kullanıcıların oluşturdukları metin tabanlı şifreleri hecelerin sırasını farklı hatırladıkları için sisteme doğru olarak girememişlerdir ve sanki şifreyi hiç hatırlamamış gibi değerlendirilmişlerdir. Grafik tabanlı şifrelerdeki amaç ezberi ortadan kaldırmaktır.

Kullanıcı bir resme baktığında iki cevabı olabilecek bir soruya cevap verecektir, soru şudur “bu resmi seçmiş miydim?”, cevap da “evet, seçtim” ya da “hayır, seçmedim” şeklindedir. Bilgisayar bilimlerinin temel mantığındaki gibi; öngörülen kimlik doğrulama sistemi ikili bir bilgi üzerinde inşaa edilmiştir. Bu tercih şifre uzayının küçülmesine neden olmaktadır; fakat yine bir ödünleşim sözkonusudur maksat yanlış negatifleri azaltmaktır.

Grafik tabanlı şifrelerin kullanıcı deneyimi henüz olgunlaşmamıştır, iki kimlik doğrulama yöntemini karşılaştırırken bu durumu hesaba katmak gerekir. Kullanıcılar henüz seri bir şekilde grafik tabanlı şifreyi girebilecek durumda değillerdir. Metin tabanlı şifreleri kullanma geçmişleri daha fazladır, iki kimlik doğrulama yöntemi karşılaştırılırken şifreyi seri bir şekilde girebilme süresini değerlendirirken bu durum da hesaba katılmalıdır. Kullanıcıların göz ve el koordinasyonunu daha iyi bir şekilde kurmaları için grafik tabanlı kimlik doğrulama yöntemini daha sıklıkla kullanmaları gerekmektedir.

4.2 Omuz Sörfüne Dirençli Olma Özelliğinin Eklenmesi

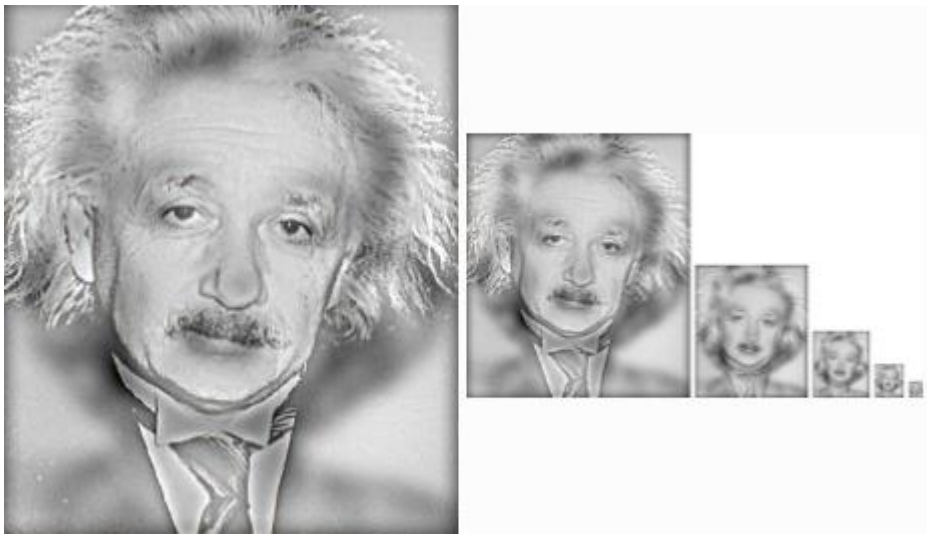
Öngörülen kimlik doğrulama yöntemine omuz sörfüne karşı dirençli olma özelliği eklenebilmektedir; bu özellik açılıp kapatılabilir niteliktedir. Yöntemin omuz sörfüne dirençli olması için en temel anlamıyla kullanıcı baktığında farklı resimleri görmelidir, arkadan ya da uzaktan bakan birisi farklı resimleri görmelidir. Hibrit resimler tam olarak bu özelliğe sahiptirler. Sistemdeki 5x5’lik resim kümesi başka 25 resimle hibritlenerek saklanabilir. Tasarlanan sistem varsayılanda omuz sörfüne dirençlidir; omuz sörfüne dirençli kimlik doğrulama ekranı açılır ve bu ekranda seçimler hibrit resimler üzerinden yapılır. Kullanıcı izlendiğini düşünmediği, kendisini güvende hissettiği bir yerde “Güvenli Bir Yerdeyim” seçeneği aracılığıyla hibrit olmayan orijinal resimler üzerinden seçimlerini yapabilir; bu durumda omuz sörfüne dirençsiz kimlik doğrulama yapılmış olur. Kullanıcı bu ekranda “Güvensiz Bir Yerdeyim” seçeneği aracılığıyla omuz sörfüne dirençli kimlik doğrulama ekranına tekrar dönebilir. Alternatif omuz sörfüne dirençli grafik tabanlı kimlik doğrulama yöntemi temel anlamda kullanılan resimlerin hibritleriyle değiştirilmesi üzerinden yürümektedir.

Omuz sörfüne karşı dirençli giriş ekranında kullanıcı hibrit resimler içerisinden seçimler yapacaktır; fakat burada önemli birkaç husus vardır? Teoride her resim başka bir resimle hibritlenebilir; fakat üretilen resimler omuz sörfü problemini aşmada başarılı olur mu? Resimlerin ideal boyutları ne olmalıdır? Resimler aynı boyutta mı olmalıdır, yoksa farklı boyuttaki resimler de hibritlenebilir mi? Resimler siyah beyaz mı olmalıdır yoksa renkli mi olmalıdır? Hibrit resimler oluşturulurken hangi araçlardan faydalanılmalıdır? Otomatik olarak çok sayıda hibrit resim üretilebilir mi? Bu araçlar hibrit resimleri üretirken hangi parametreleri hangi değerlerde kullanmaktadırlar? Hibritleme işlemi matematiksel olarak resimler üzerinde nasıl yapılmaktadır? Yanlış negatifler ve yanlış pozitifler nasıl azaltılabilir? Bu tez çalışması kapsamında bu soruların cevapları aranmaktadır.

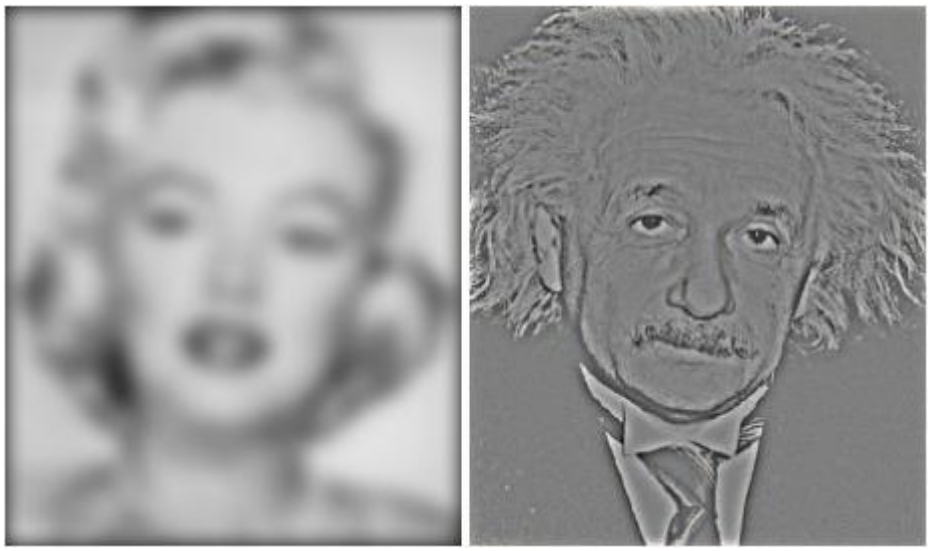
Hangi tip resimlerin birbirlerine eklendiklerinde diğerini daha iyi saklayacağına dair bazı çalışmalar yapılmıştır (Miyachi 2010, Takahashi vd. 2011). Bu çalışmalar; bu tez çalışmasında öngörülen görsel şifre tekniğinde faydalı olmamaktadır. Örneğin fasulye tanesi ile böbrek resimleri kullanılarak hibrit bir resim oluşturulabilir; bunlar birbiri üzerine çok iyi oturtulabilmektedir. Yakından bakan kullanıcı fasulye görürken uzaktan bakan omuz sörfü yapan kötü niyetli kişi böbrek görebilir ve şifrenin böbrek resmini içerdiğini sanabilir; fakat bir süre sonra omuz sörfü yapan kişi kendisi de sisteme kayıt olursa böbrek ile fasulyenin eşleştiğini bilir ve böbrek gördüğünde bunun aslında fasülye olduğunu anlayabilir. Bu istenen bir durum değildir; dolaylı yoldan da olsa omuz sörfüyle doğru şifre parçası öğrenilmiş olunur. Öngörülen grafik şifre sisteminde uzaktan böbrek gördüğünde bunun aslında fasülye olduğunu omuz sörfü yapan kişi bilememelidir; başka ihtimaller de olmalıdır. Bu durumda iki seçenek kalmaktadır: ya bir resme benzeyen birden fazla resim olmalıdır ya da benzeme gibi bir özellik aranmayıp bir resim başka birçok resimle hibiritlenebilmelidir. Böbrek ve fasülye ikilisine 3.,4.,5. ve daha fazla sayıda benzerlerin eklenmesi güçtür ve bu durumda küçük bir şifre uzayı elde edilmektedir; bu sebeple benzerlik aramaksızın sistematik bir şekilde bir resmi başka n tane resimle hibritleyebilmek gerekmektedir.

4.3 Sistematik Olarak Hibrit Resimlerin Üretilmesi

Bir resmin düşük uzaysal frekansları ile başka bir resmin yüksek uzaysal frekanslarının birbirine eklenmesi sonucu hibritler resimler elde edilmektedir. Şekil 4.10'da ölçeklenmiş bir hibrit resim örneği verilmiştir. Resim orijinal boyutundayken Albert Einstein, küçültüldüğünde Marilyn Monroe gözükmektedir. Resim elde edilirken Marilyn Monroe resmi düşük frekansları geçiren bir filtreden, Albert Einstein resmi ise yüksek frekansları geçiren bir filtreden geçirilmiştir (Şekil 4.11).



Şekil 4.10 Hibrit resim örneği



Şekil 4.11 Filtrelerden geçirilmiş Marilyn Monroe ve Albert Einstein

Herhangi iki resim hibritlenirken aynı boyutta olmaları gerekmektedir. Resimler hibritlenirken bu hususa dikkat edilmelidir. Şekil 4.11'deki hibrit resimler MATLAB ortamında üretilmiştir. Matematiksel olarak Marilyn Monroe ve Albert Einstein resimleri hibritlenirken şu işlemler yapılmıştır:

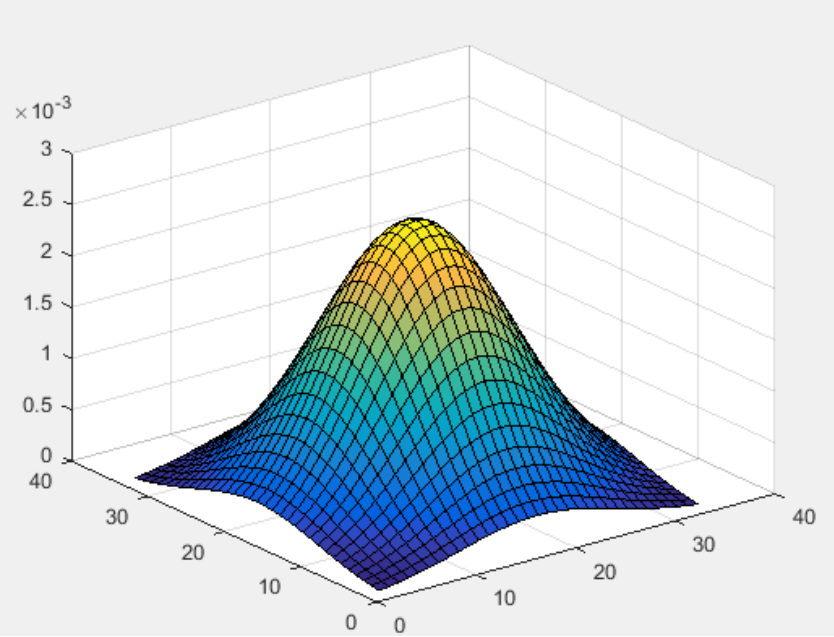
- Resimlerin grilik skalası (grayscale) içerisinde olması sağlanmıştır.
- Marilyn Monroe resminin değerleri, 0 ve 1 arasında değişecek şekilde R1 matrisine atanmıştır.
- Albert Einstein resminin değerleri, 0 ve 1 arasında değişecek şekilde R2 matrisine atanmıştır.
- Düşük uzaysal frekansları geçiren bir filtre matrisi G belirlenmiştir. Düşük frekansları geçiren filtrelerden en bilineni Gauss filtresidir. Gauss filtresi matrisi oluşturulurken matrisin 33'e 33'lük olması ve değerlerinin standart sapmasının 8 olması uygun bulunmuştur.
- R1 matrisi G filtresinden geçirilip, A1 matrisi elde edilmiştir: A1 = R1.G
- R2 matrisi G filtresinden geçirilmiştir, A2 matrisi elde edilmiştir: A2 = R2.G
- A2 matrisi Einstein resminin düşük frekanslı biçimidir, fakat bunun tam tersi yüksek frekanslı biçimi hesaplanmalıdır. Bu sebeple R2 matrisinden A2 matrisi çıkarılıp Y2 matrisi elde edilmiştir.

- A1 (düşük frekanslı Marlin resmi) ile Y2 (yüksek frekanslı Einstein resmi) üstüste eklendiğinde hibrit resim matrisi H elde edilmiştir: H = A1+Y2

Belirlenen algoritma MATLAB ortamında aşağıdaki metotları kullanarak uygulamaya geçirilmiştir:

```
R1 = im2single(imread(['Marilyn'.jpg']));
R2 = im2single(imread(['Einstein.jpg']));
kesmeFrekansi = 8;
filtre = fspecial('Gaussian', kesmeFrekansi*4+1,
kesmeFrekansi);
A1 = imfiltre(R1, filtre);
A2 = imfiltre(R2, filtre);
high_frequencies = double(R2) - A2;
hybrid_image = imadd(high_frequencies,A1);
imwrite(hybrid_image, ['Hibrit.jpg'], 'quality', 95);
```

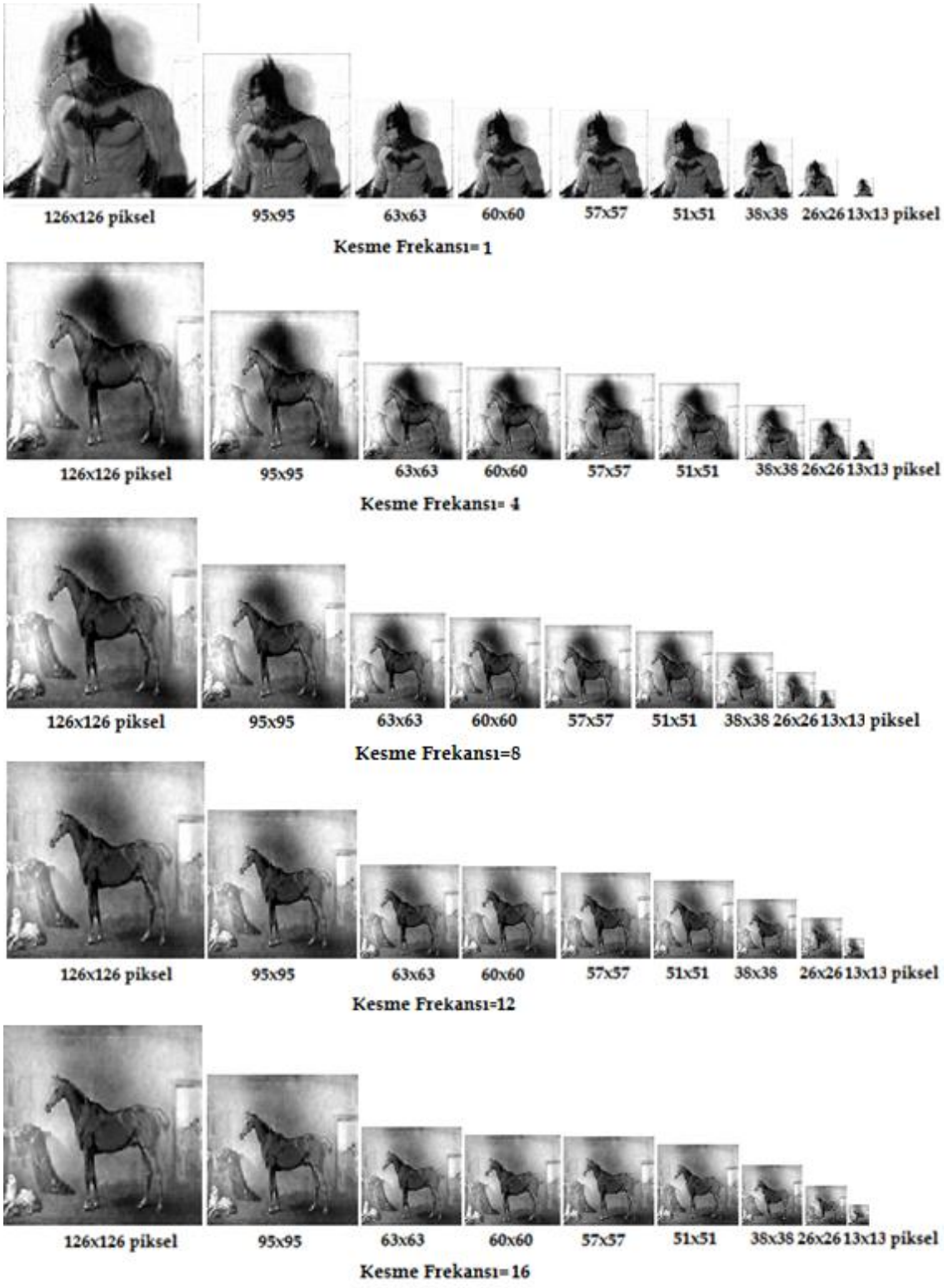
MATLAB'ın fspecial fonksiyonun parametrelerine verilen değerler tamamen buluşsal (heuristics) olarak seçilmiştir. Kesme frekansı (cutoff frequency) oluşturulacak filtre matrisinin standart sapmasını temsil etmektedir. Filtre matrisinin +2Xkesme frekansı ile -2Xkesme frekansı aralığında ideal komşuluk değerlerine sahip olacağı varsayımı ile boyutu (kesme frekansıX4)+1 olarak belirlenmiştir. Kesme frekansı 8 verildiğinde oluşan filtrenin gösterimi şekil 4.12'deki gibidir.



Şekil 4.12 Kesme frekansı 8 olarak belirlenmiş Gauss filtresi matrisi

Hibrit resimler oluşturulurken temel olarak Marilyn Monroe ve Albert Einstein resimlerine uygulanan işlemler takip edilmektedir. Resimler seçilirken siyah beyaz olmalarına ya da grilik skalasından (grayscale) geçirilmiş hallerinin kullanılmasına dikkat edilmektedir. Renk faktörü hibrit resimleri yorumlarken çok güçlü bir ipucu oluşturmakta ve resimlerin birbirlerini saklamalarını güçleştirmektedir (Oliva 2006).

Kullanıcı şifre giriş ekranında 25 tane resmin ekrana rahatlıkla sığabilmesi için boyut olarak 126x126 piksel boyutları uygun bulunmuştur. İlk aşamada oluşturulan hibrit resimler de bu boyutlarda oluşturulmuştur; fakat bu boyutta oluşan resimler kullanıcının şifresini oluşturan asıl resim kümesini saklamakta başarısız olmuştur. Optimum resim boyutunu belirlemek için değişik boyutlarda hibrit resimler oluşturulmuştur (Şekil 4.13). Resim başarısı üzerinde etkili olan bir diğer parametre de kesme frekansıdır; bu parametre değiştirildiğinde hibrit resimler ciddi oranda değişmektedir (Şekil 4.13). Kesme frekansı arttıkça örneğin 16 alındığında, düşük frekanslı filtreden geçen resimler hibrit resimde görünmemektedir. Yüksek kesme frekansında oluşturulan hibrit resimler

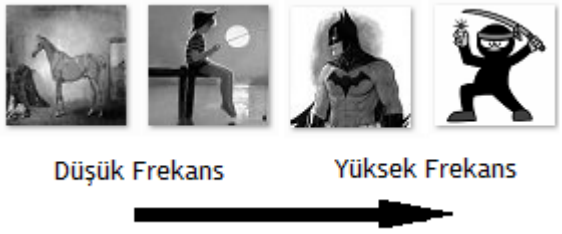


Şekil 4.13 Değişik boyutlarda ve kesme frekanslarında oluşturulmuş hibrit resimler

kullanıcı giriş ekranında kullanıldığında kullanıcı doğru resmi görür; fakat ekranı gören birisi de aynı resmi görür ve bu durumda yanlış pozitiflerin sayısı artacaktır. Kesme frekansı düştükçe de, örneğin 1 alındığında yüksek frekanslı filtreden geçirilmiş olan resimler görünmemektedir. Bu durumda oturumu izleyen kişi açısından yöntem doğru çalışır; fakat geçerli kullanıcı kendi şifresinde bulunan resmi görememiş olur ve yanlış negatiflerin sayısı artacaktır. Bu da istenmeyen bir durumdur. Kesme frekansı 8 olarak orta bir değer alındığında istenilen özellikle resimler üretilebilmektedir. Optimum kesme frekansı değeri ampirik olarak belirlenmiştir.

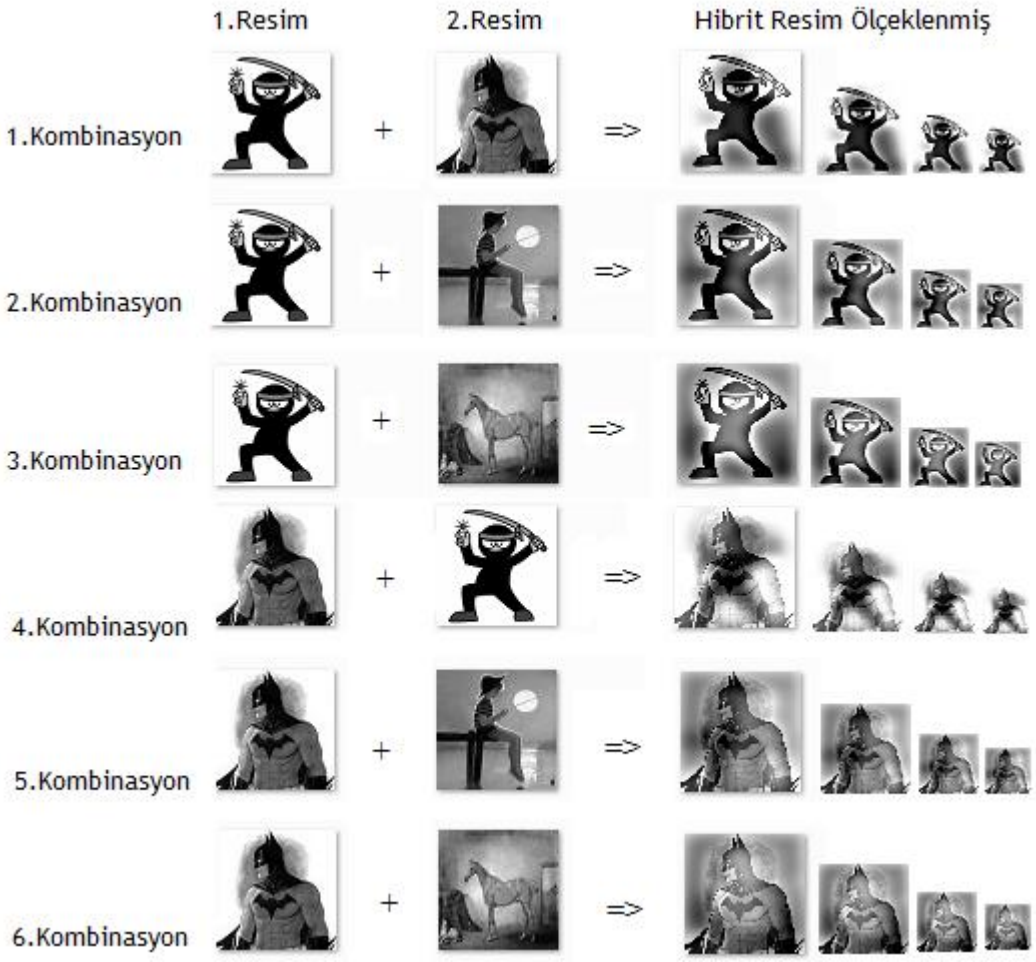
Resim boyutu omuz sörfüne dirençsiz olan durumdaki gibi 126x126 olarak kullanılırsa ekranı izleyen birisi de bu resmi kolaylıkla algılayabilmektedir, resmin küçültülmesi hibrit özelliğinin daha ön plana çıkmasını sağlayacaktır ve sistemi izleyen birisiyle geçerli kullanıcı farklı resimleri göreceklerdir. Piksel boyutları 60x60 olarak alındığında istenilen özellikle resimler üretilebilmektedir (Şekil 4.13).

Kesme frekansının ve resim boyutlarının ideal değerleri belirlendikten sonra üzerinde durulması gereken başka bir husus daha bulunmaktadır. Bu husus da hangi tip resimlerin kullanılacağıdır. Teorik olarak herhangi aynı boyuttaki iki resim hibritlenebilmektedir; fakat yakından bakıldığında farklı uzaktan bakıldığında farklı görünme konusunda hepsi başarılı olamamaktadır. Belli bir sistematiğe oturtularak hibrit resimler üretilebilmelidir. Tasarlanan kullanıcı giriş ekranında; sadece geçerli kullanıcının görmesi beklenen resimler bir grup içerisinden, oturumu izleyen birisinin görmesi beklenen resimler de başka bir grup içerisinden rastgele seçilip hibritlenerek kullanıcıya sunulabilir. Bu şekilde sistematik olarak hibrit resimler üretilmiş olur. Bu iki grup da 25'er resimden oluşmalıdır ve resimler yanlış negatifleri ve yanlış pozitifleri minimuma çekebilmelidir. Grupların belirlenmesi için 2 yüksek frekanslı, 2 alçak frekanslı resim seçilmiştir ve frekans değerlerine göre artan şekilde sıralanmıştır (Şekil 4.14).



Şekil 4.14 Değişik frekanslarda 4 adet siyah beyaz resim

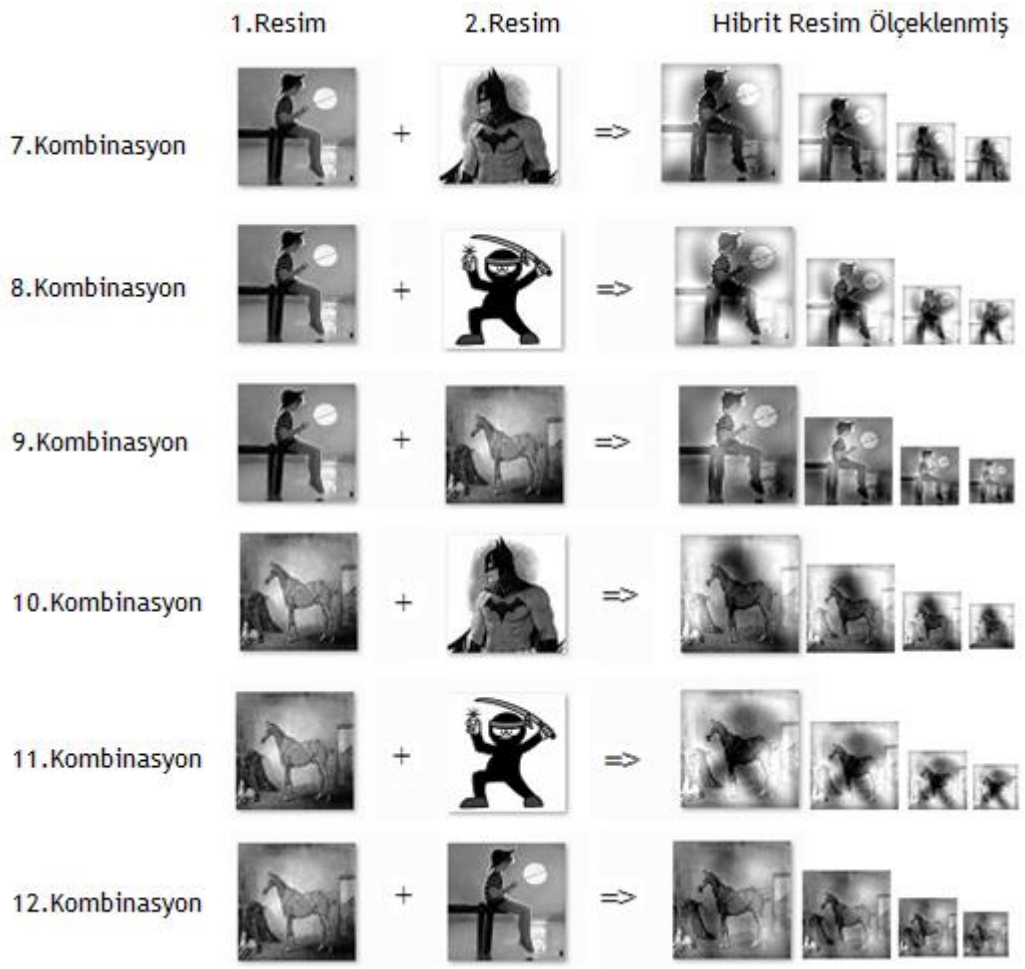
Yüksek frekanslı resimler daha keskin geçişlere sahipken, alçak frekanslı resimler daha yumuşak geçişlere sahiptir. Bu 4 resmin birbirileriyle her kombinasyonu içerecek



Şekil 4.15 Üretilen hibrit resimler

şekilde hibritlenmesi sonucu şekil 4.15-4.16'daki hibrit resimler elde edilmiştir. Hibrit resimler elde edilirken birinci resim yüksek frekansları geçiren bir filtreden, ikinci resim

de alçak frekansları geçiren bir filtreden geçirilmiştir. Yüksek frekansları geçiren filtreden yüksek frekanslı resim geçirilip, düşük frekansları geçiren filtreden düşük frekanslı resim geçirildiğinde şekil 4.16'daki 2., 3., 5. ve 6. kombinasyonlar elde edilmiştir. Bu dört kombinasyonda elde edilen hibrit resimler



Şekil 4.16 Üretilen hibrit resimlerin devamı

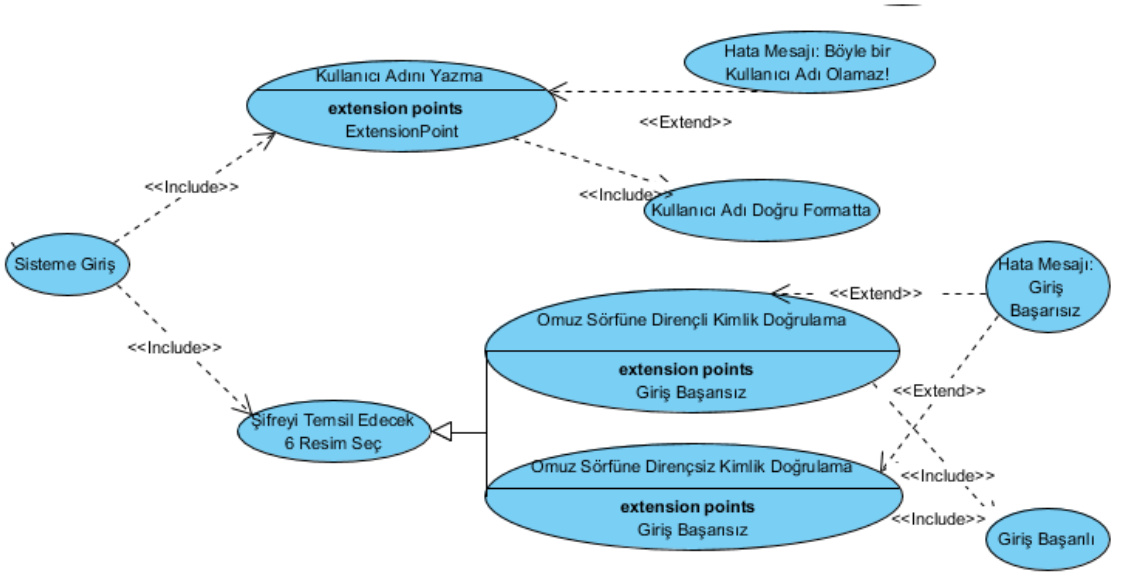
istenen özellikte değildir. Üretilen hibrit resme yakından bakıldığında da uzaktan bakıldığında da baskın olarak birinci resim görünmektedir. 1.kombinasyonda gösterildiği üzere iki yüksek frekanslı resim kullanılarak hibrit resim üretilmek istendiğinde ise daha yüksek frekanslı olan yüksek frekansları geçiren filtreden, daha alçak frekenslı olan alçak frekansları geçiren filtreden geçirildiğinde sonuç yine istenen özellikte değildir. Oluşan hibrit resim yakından da uzaktan da aynıdır. Yine iki yüksek

frekanslı resim 1. kombinasyonun tersi sırada filtrelerden geçirildiğinde 4. kombinasyondaki hibrit resim üretilmektedir. Üretilen hibrit resim beklenen özelliğe sahiptir. Yakından bakıldığında farklı uzaktan bakıldığında farklı gözükmektedir. Bu altı kombinasyon göz önüne alındığında şöyle bir çıkarım yapılabilir: "iki resimden hangisi daha yüksek frekansta ise o resmi alçak frekansları geçiren filtreden, hangisi daha alçak frekansta ise o resmi de yüksek frekansları geçiren filtreden geçirmek suretiyle başarılı hibrit resimler üretilebilir." Bu çıkarımdan yola çıkarak şekil 3.16'daki 9.kombinasyon dışında tüm kombinasyonlarda üretilen hibrit resimlerin başarılı olması beklenir. 9. kombinasyonda istenen sonuç alınamamıştır; çünkü ikinci resim tamamen yokolmuştur, yakından da uzaktan da resmin yorumu aynıdır. Bu istenen bir durum değildir 7., 8. , 10. , 11., 12 kombinasyonlarda üretilen resimler elde edilen çıkarımı doğrulamaktadır. Bir diğer dikkat çekici husus da iki resmin arasında ne kadar frekans farkı varsa üretilen hibrit resimler o derecede başarılı olmaktadır. Daha başarılı hibrit resim elde etmek için yüksek frekenslı resim, daha yüksek frekanslı resim ya da alçak frekanslı resim, daha alçak frekanslı resim kombinasyonları yerine doğrudan yüksek frekanslı resim ile alçak frekanslı resim kombinasyonları seçilebilir. Yüksek frekanslılar bir gruba, alçak frekanslılar diğer gruba atanabilir.

Tasarlanan kullanıcı giriş ekranında; sadece geçerli kullanıcının görmesi beklenen resimler alçak frekanslı resimler kümesinden, oturumu izleyen birisinin görmesi beklenen de yüksek frekanslı resimler kümesinden seçilmek suretiyle hibritlenerek kullanıcıya sunulabilir.

5. ÖNERİLEN YÖNTEMİN UYGULANMASI

Sistematik olarak hibrit resimlerin üretilmesi sonucu öngörülen alternatif kimlik doğrulama yöntemi hayata geçirilebilir. Bölüm 4.2'de kurgulandığı üzere yöntemin omuz sörfüne dirençli olma özelliği açılır, kapanır nitelikte düşünülmüştür. Kullanıcı öngörülen kimlik doğrulama yöntemi içerisinde şekil 5.1'deki UML kullanım durumu diyagramındaki (Use Case Diagram) gibi hareket edebilmektedir.

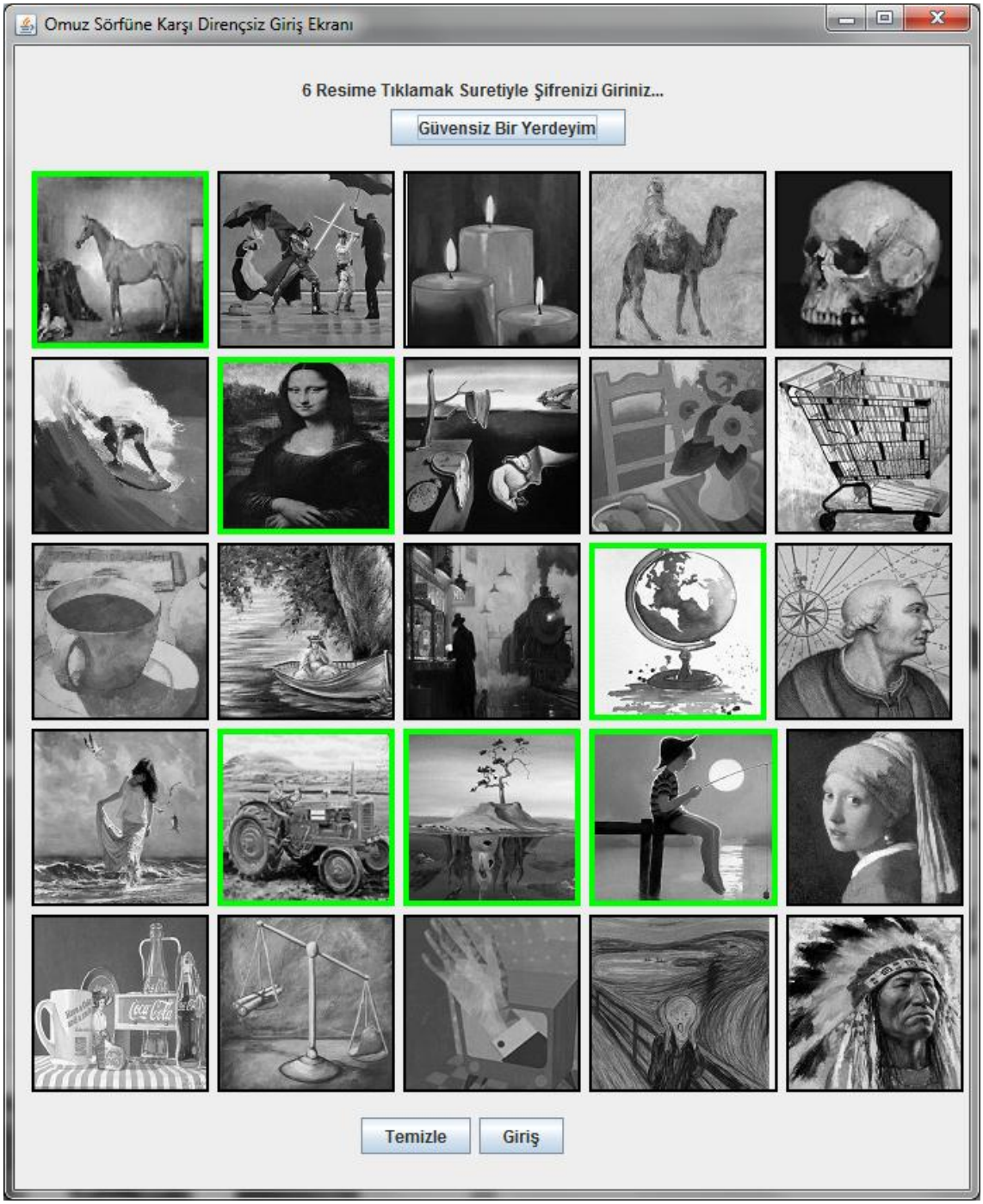


Şekil 5.1 Öngörülen yöntemin kullanım durumu diyagramı

Kullanıcı sisteme kayıt aşamasını tamamladıktan sonra sisteme giriş yapmak istediğinde benzersiz kullanıcı adını doğru yazmalıdır ve kayıt olurken seçtiği 6 resmi tekrar hatırlayıp seçebilmelidir. Kullanıcı seçimlerini orijinal kayıtta seçtiği resimler üzerinden ya da bu resimlerin başka resimlerle hibritlenmiş halleri üzerinden yapmalıdır. Uygulamada kullanılmak üzere alçak frekanslı ve yüksek frekanslı 25'lik iki resim kümesi belirlenmiştir. Sistematik olarak MATLAB yardımı ile 25x25=625 adet hibrit resim oluşturulmuştur ve her bir hibrit resim 1<=i<=25, 1<=j<=25 olmak üzere Resim_i_Karakter_j şeklinde uygulamanın arka planında temsil edilmiştir. Sistem omuz sörfüne dirençli kimlik doğrulama ekranını oluştururken her i değeri için bir j değeri bularak bu iki indekse denk gelen hibrit resmi resim veritabanından almıştır.

Şekil 5.2 Omuz sörfüne dirençli kimlik doğrulama ekranı

Orijinal resimler üzerinden gerçekleşen kimlik doğrulama omuz sörfüne dirençsizdir, hibrit resimler üzerinden gerçekleşen kimlik doğrulama ise omuz sörfüne karşı dirençlidir. Uygulama varsayılan olarak omuz sörfüne dirençli kimlik doğrulama ekranı gelecek şekilde kurgulanmıştır (Şekil 5.2). Kullanıcı bu ekranda "Güvenli Bir Yerdeyim" butonuna basarak resimlerin orijinal halleri üzerinden omuz sörfüne



Şekil 5.3 Omuz sörfüne dirençsiz kimlik doğrulama ekranı

dirençsiz bir şekilde kimlik doğrulama yapmayı tercih edebilir (Şekil 5.3). Yine şekil 5.3'de görüldüğü üzere omuz sörfüne dirençsiz kimlik doğrulama ekranında iken "Güvensiz Bir Yerdeyim" butonuna basarak tekrar omuz sörfüne dirençli kimlik doğrulama ekranına geçebilir.

Veritabanında kullanıcının şifresine denk gelen resim indeksleri adrese dayalı hesaplama (hashing) işleminden geçirilmiş olarak tutulmaktadır. Kimlik doğrulama ekranlarında seçilen i değerlerinin adrese dayalı hesaplama ile elde edilen değerleri veritabanındaki ile karşılaştırılmak suretiyle kullanıcının şifresinin doğruluğundan emin olunmaktadır. Veritabanında tutulan değerden şifreye ulaşmak mümkün değildir, çünkü adrese dayalı hesaplama işlemi tek yönlü çalışır. Bu da sistemin bir güvenlik katmanı oluşturmak adına aldığı diğer bir önlemdir.

Bir diğer önemli husus da omuz sörfü yapan kişinin ekranı hangi uzaklıktan görebileceğine dair bir uzaklık değeri belirleyebilmektir. Omuz sörfüne dirençli kimlik doğrulama ekranında orijinal resimleri görebilmek için kullanıcının ekrana yaklaşması gerekmektedir; çünkü bazı detaylar ancak yakından daha net anlaşılabilmektedir. Geçerli kullanıcı istemsiz olarak ekrana yaklaşarak seçimlerini yapmak durumundadır. Omuz sörfü yapan geçerli olmayan kullanıcı da da 1 ila 1.5 metre uzaklıktan ekranı görebilir, resimlerin boyutlarına buluşsal (heuristic) olarak karar verirken 1.5 metre uzaklıkta omuz sörfü yapan biri olduğu varsayımı yapılmıştır. Son durumda, hibrit resimlerin boyutları 60x60 piksel, orijinal resimlerin boyutları 126x126 piksel, omuz sörfü uzaklıklığı da 150 cm olarak belirlenmiştir.

Bilgisayar kullanımı konusunda deneyimli 30 kullanıcı belirlenip önerilen yöntem üzerinde bir kullanıcı deneyimi araştırması yapılmıştır. Her kullanıcı sistemde hem geçerli kullanıcı statüsünde hem de omuz sörfü yapan geçerli olmayan kullanıcı statüsünde çalışmaya katkıda bulunmuşlardır.

5.1 Sisteme Kayıt ve Belirlenen Şifreleri Aralıklarla Sisteme Girme

Kullanıcılar öncelikle sisteme kayıt olmuşlardır. Kullanıcılar sisteme kayıt olurken aynen bölüm 4.1.1'deki yönergeleri izlemişler. 30 kullanıcı benzersiz kullanıcı adlarını ve şifrelerini temsil edecek 6 uzunluktaki resim şifrelerini belirlemişlerdir. Kullanıcılardan şifrelerini oluşturduktan sonra omuz sörfüne dirençsiz kimlik doğrulama ekranında şifrelerini girmeleri istenmiştir. Kullanıcılar şifrelerini 5 kere doğru girene kadar denemelerde bulunmuşlardır. Sisteme kayıttan bir hafta sonra

kullanıcılardan şifrelerini sisteme 5 kere doğru girmeleri beklenmiştir ve 15 gün sonra da aynı şekilde yine şifrelerini sisteme girmeleri istenmiştir. Kullanıcılardan şifresini doğru hatırlamayanlar olduğunda şifremi göster ekranı açılıp, sonrasında tekrar şifrelerini sisteme girmeleri istenmiştir. Bu alıştırmalardaki amaç kullanıcıların metin tabanlı şifreyi kullandıkları sıklıkla resim tabanlı şifrelerini kullanmış olmalarını sağlamaktır. Bu alıştırmalar şekil 5.1'deki omuz sörfüne dirençsiz kimlik doğrulama ekranı üzerinde gerçekleştirilmiştir.

5.2 Omuz Sörfüne Dirençli Kimlik Doğrulama

Kullanıcılar; omuz sörfüne dirençsiz kimlik doğrulama ekranında yapılan çok sayıda denemelerden sonra şifrelerini adeta uzun süredir kullandıkları metin tabanlı şifrelerini girdikleri serilikte ve hızda girebilir duruma gelmişlerdir. Sonraki aşamada kullanıcılardan omuz sörfüne dirençli ekranda şifrelerini girmeleri beklenmiştir. Kullanıcılar her grup 5 kişiden oluşacak şekilde 6 ayrı gruba ayrılmıştır. Her grup bir veri setine tekabül edecek şekilde düşünülmüştür. Bu veri setleri üzerinden yanlış-pozitiflik, yanlış-negatiflik, doğru-pozitiflik, doğru-negatiflik sayıları ve doğruluk oranı elde edilmek istenmiştir. Grubu oluşturan 5 kişi de omuz sörfüne dirençli kimlik doğrulama ekranında şifresini girmiştir. İlk kişi şifresini girerken diğer 4 kişi oturumu izlemiştir ve ilk kişinin şifresini girmesinin ardından diğer 4 kişi ilk kişinin şifresini hatırlayabildiği kadarıyla omuz sörfüne dirençsiz ekranda girmiştir. Sonrasında ikinci kişi, üçüncü, dördüncü ve beşinci kişiler için aynı yöntem izlenmiştir. İlk grubu diğer gruplar izlemiştir ve her bir grupta 20 toplamda 120 kere olmak üzere şifre denemesi yapılmıştır. Şifreyi giren kullanıcı ekrana maksimum miktarda yaklaşabilecekken, omuz sörfü yapacak olan kullanıcı 1.5 metre geriden oturumu izleyebilmiştir. Tüm oturumlarda bu 1.5 metre kuralına uyulmuştur. Yapılan denemelerde elde edilen veriler tablolaştırırken her bir kullanıcı şifresine karşılık her bir kullanıcının ilgili şifreyi bilip bilemememe durumu göz önüne alınmıştır. Örneğin 1. grupta 1. kullanıcının şifresini 1.kullanıcının doğru bilmesi, diğer kullanıcıların yanlış bilmesi beklenmiştir. Bir kullanıcının şifresini bilmesi gereken bir kullanıcı bildiğinde bu durum TP ile, bir kullanıcının şifresini bilmesi gereken bir kullanıcı bilemediğinde bu durum FN ile, bir kullanıcının şifresini bilmemesi gereken bir kullanıcı bildiğinde bu durum FP, bir

kullanıcının şifresini bilmemesi gereken bir kullanıcı bilemediğinde bu durum TN ile tablolarda temsil edilmiştir. 1.grup için 20 şifre denemesinin sonucu çizelge 5.1'deki gibidir. Benzer şekilde her bir grup için elde edilen değerler takip eden çizelgelerdeki gibidir. (Çizelge 5.2-5.6)

Çizelge 5.1 1. grup için TP, TN, FP,FN değerleri

Şifre\Şifreyi Giren	1.Kullanıcı	2.Kullanıcı	3.Kullanıcı	4.Kullanıcı	5.Kullanıcı
1.Kullanıcının Şifresi	TP	TN	TN	TN	TN
2.Kullanıcının Şifresi	TN	FN	TN	TN	TN
3.Kullanıcının Şifresi	TN	TN	TP	TN	TN
4.Kullanıcının Şifresi	TN	TN	FP	TP	TN
5.Kullanıcının Şifresi	TN	TN	TN	TN	TP

Çizelge 5.2 2. grup için TP, TN, FP,FN değerleri

Şifre\Şifreyi Giren	1.Kullanıcı	2.Kullanıcı	3.Kullanıcı	4.Kullanıcı	5.Kullanıcı
1.Kullanıcının Şifresi	TP	TN	TN	TN	TN
2.Kullanıcının Şifresi	TN	TP	TN	TN	TN
3.Kullanıcının Şifresi	TN	TN	TP	TN	TN
4.Kullanıcının Şifresi	FP	TN	FP	TP	TN
5.Kullanıcının Şifresi	TN	FP	TN	TN	TP

Çizelge 5.3 3. grup için TP, TN, FP,FN değerleri

Şifre\Şifreyi Giren	1.Kullanıcı	2.Kullanıcı	3.Kullanıcı	4.Kullanıcı	5.Kullanıcı
1.Kullanıcının Şifresi	TP	TN	TN	TN	TN
2.Kullanıcının Şifresi	TN	TP	TN	FP	TN
3.Kullanıcının Şifresi	TN	TN	TP	TN	TN
4.Kullanıcının Şifresi	TN	TN	TN	TP	TN
5.Kullanıcının Şifresi	FP	TN	TN	TN	TP

Çizelge 5.4 4. grup için TP, TN, FP,FN değerleri

Şifre\Şifreyi Giren	1.Kullanıcı	2.Kullanıcı	3.Kullanıcı	4.Kullanıcı	5.Kullanıcı
1.Kullanıcının Şifresi	TP	TN	TN	TN	TN
2.Kullanıcının Şifresi	TN	FN	FP	TN	TN
3.Kullanıcının Şifresi	TN	TN	TP	TN	TN
4.Kullanıcının Şifresi	TN	TN	TN	FN	TN
5.Kullanıcının Şifresi	FP	FP	TN	TN	TP

Çizelge 5.5 5. grup için TP, TN, FP,FN değerleri

Şifre\Şifreyi Giren	1.Kullanıcı	2.Kullanıcı	3.Kullanıcı	4.Kullanıcı	5.Kullanıcı
1.Kullanıcının Şifresi	TP	TN	TN	TN	TN
2.Kullanıcının Şifresi	TN	TP	FP	TN	TN
3.Kullanıcının Şifresi	TN	TN	TP	TN	TN
4.Kullanıcının Şifresi	TN	TN	TN	TP	TN
5.Kullanıcının Şifresi	FP	TN	TN	TN	FN

Çizelge 5.6 6. grup için TP, TN, FP,FN değerleri

Şifre\Şifreyi Giren	1.Kullanıcı	2.Kullanıcı	3.Kullanıcı	4.Kullanıcı	5.Kullanıcı
1.Kullanıcının Şifresi	TP	TN	TN	TN	TN
2.Kullanıcının Şifresi	TN	TP	FP	TN	TN
3.Kullanıcının Şifresi	TN	TN	TP	TN	FP
4.Kullanıcının Şifresi	TN	TN	TN	TP	TN
5.Kullanıcının Şifresi	TN	TN	TN	FP	TP

5.3 Verilerin Analizi

Önerilen kimlik doğrulama yöntemini kullanarak yürütülen kullanıcı deneyimi araştırmasında elde edilen TP, TN, FN, FP değerleri üzerinden bir analiz yapmak mümkündür. Her bir grup bir veri seti olarak düşünülebilir. Her bir veri seti üzerinden analiz yapılıp, yapılan analizler birleştirilip tüm 6 veri setini de kapsayan sonuç elde etmek mümkündür. İlk aşamada her bir veri seti için doğruluk oranı hesaplanabilir. Doğruluk oranı analizinde aşağıdaki formül kullanılmıştır:

$$\text{Doğruluk Oranı} = (TP+TN)/(TP+FP+FN+TN)$$

Her bir veri seti için elde edilen doğruluk oranları değerleri çizelge 5.7'deki gibidir.

Çizelge 5.7 Hesaplanan doğruluk oranı değerleri

Veri Seti	Kullanıcı Sayısı	TP	FP	FN	TN	Toplam	Doğruluk (%)
1	5	4	1	1	19	25	92%
2	5	5	3	0	17	25	88%
3	5	5	2	0	18	25	92%
4	5	3	3	2	17	25	80%
5	5	4	2	1	18	25	88%
6	5	5	3	0	17	25	88%
	Toplam	26	14	4	106	150	88%

Elde edilen veriler üzerinden bir analiz yapmak gerekirse TP+TN oranı genel olarak yüksektir. Omuz sörfüne dirençli kimlik doğrulama ekranında geçerli kullanıcıların da şifrelerini doğru giremediği durumlar olmuştur (FN); fakat genellikle geçerli şifrelerini doğru şekilde girebilmişlerdir. (TP) Benzer şekilde omuz sörfü ile başka bir kullanıcının şifresini doğru gören kullanıcılar olmuştur (FP); fakat büyük oranda omuz sörfü işlemi başarısız olmuştur (TN).

Kullanıcı deneyimi araştırmasında elde edilen tüm veriler analiz edildiğinde önerilen yöntemin omuz sörfüne dirençli bir kimlik doğrulama sunduğu kanısı güçlenmektedir. Yöntem çerçevesinde geçerli kullanıcılar şifrelerini hibrit resimler içerisinden seçebilmişlerdir, omuz sörfü yapan diğer kullanıcılar ise hibrit resimler içerisinden geçerli kullanıcının şifresini oluşturan resimleri net olarak görememişlerdir.

Tüm elde edilen veriler ışığında önerilen yöntem alternatif omuz sörfüne dirençli bir kimlik doğrulama yöntemi olarak başarılıdır ve hem masaüstü hem de android/ios sistemlerde kimlik doğrulama yöntemi olarak kullanılabilir.

6. TARTIŞMA ve SONUÇ

Günümüzde bilgi güvenliği hayati önem taşımakla beraber sağlanması gittikçe zorlaşan bir kavram olmaktadır. Bilgi güvenliği denilince akla ilk gelen alfasayısal değerlerden oluşan şifrelerdir; fakat metin tabanlı şifreler artık yetersiz kalmaktadır. Kullanıcılar daha hızlı ve daha kolay kimlik doğrulama süreci ihtiyacında iken, sistemler de daha güvenli olmak ihtiyacındadır. Bu zayıflıklarından dolayı metin tabanlı şifreler yerine grafik tabanlı şifreler kullanılabilir. İnsanların resim hafızasının, kelime ve sayılara göre daha kalıcı olduğunu gösteren çalışmalar ışığında grafik tabanlı şifreler metin tabanlı şifrelere iyi bir alternatif olarak değerlendirilmektedir. Grafik tabanlı şifreler için de güncelliğini koruyan en büyük problem omuz sörfüdür. Bu çalışmada omuz sörfü problemine de çözüm arayan alternatif bir grafik tabanlı kimlik doğrulama yöntemi üzerinde durulmuştur. Alternatif yöntem oluşturulmadan önce mevcut grafik tabanlı kimlik doğrulama yöntemleri üzerinde durulup, bir altyapı oluşturulmak istenmiştir. Sonrasında alternatif yönteme özgünlük katabilecek, diğer yöntemlerin üstüne eklenebilecek yönü ne olabilir sorusu üzerinde durulmuştur. Çözüm olarak da normal resimler yerine hibrit resimler kullanma fikri öne atılmıştır. Hibrit resimleri kullanmak teorik olarak omuz sörfü problemine gayet iyi bir çözümdür. Bu düşünceden yola çıkılarak hibrit resimleri kullanan omuz sörfüne dirençli kimlik doğrulama yöntemi önce teoriksel olarak tasarlanmış sonrasında bir uygulama aracılığıyla hayata geçirilmiştir. Hibrit resimleri kullanma fikri hayata geçirilirken birçok hesaba katılmayan parametre devreye girmiştir. Her resim başka bir resimle başarılı bir hibrit resim oluşturabilir mi? Hibrit resimlerin boyutları ne olmalıdır? Hibrit resimler renkli mi olmalıdır, yoksa siyah beyaz mı olmalıdır? Geçerli kullanıcı hibrit resimlere baktığında orijinal resmi kolaylıkla görebilmekte midir? Omuz sörfü yapan kullanıcıdan gerçek resim iyi saklanabilecek şekilde mi hibrit resimler üretilmiştir? Omuz sörfü yapan kullanıcı ekrana hangi mesafede durmuştur? Otomatik olarak büyük bir hibrit resim veritabanı oluşturulabilir mi? Çalışmanın en çok üzerinde durulan ve daha da durulmaya gerek duyulan kısmı hibrit resim fenomenidir. Bu tez çalışmasında ortaya konulan uygulamada kullanılan hibrit resimlerin teorisinde ve pratiğinde bazı iyileştirmeler yapılarak daha başarılı bir omuz sörfüne dirençli grafik tabanlı kimlik doğrulama sistemi geliştirilip, yaygın olarak kullanılabilir.

KAYNAKLAR

Adams, A. and Sasse, M. A. 1999. Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures. Communications of the ACM, 42(12), 41-46.

Anderson, R. 1993. Why cryptosystems fail. In Proceedings of the 1st ACM Conference on Computer and Communications Security (215-227). ACM.

Anonymous 1996. Web Sitesi: http://www.passlogix.com, Erişim Tarihi: 10.06.2005.

Anonymous 2005. Web Sitesi: http://www.realuser.com, Erişim Tarihi: 15.03.2018.

Anonymous 2012. Web Sitesi: https://www.huffingtonpost.com/2012/10/24/facial-recognition-brain-fusiform-gyrus_n_2010192.html Erişim Tarihi: 04.03.2018

Anonymous 2017. Web Sitesi: Collection of 1.4 Billion Plain-Text Leaked Passwords Found Circulating Online Web Sitesi: https://thehackernews.com/2017/12/data-breach-password-list.html. Erişim Tarihi: 22.04.2018.

Bagchi, A. and Atluri, V. 2006. Information Systems Security: Second International Conference (ICISS 2006), 19-21 December, Proceedings (Lecture Notes in Computer Science / Security and Cryptology), 43-44, Kolkata, India.

Bhanushali, A., Mange, B., Vyas, H., Bhanushali, H. and Bhogle, P. 2015. Comparison of graphical Password authentication techniques. International Journal of Computer Applications, 116(1).

Blonder, G. E. 1996 Graphical passwords. Lucent Technologies, Inc. , Murray Hill, NJ, U. S. Patent, Ed.United States.

Bonnar, L., Gosselin, F. and Schyns, P. G. 2002. Understanding Dali's Slave Market with the Disappearing Bust of Voltaire: a case study in the scale information driving perception, Perception 31, 683–691.

Brady, T. F. and Oliva, A. 2012. Spatial frequency integration during active perception: perceptual hysteresis when an object recedes, Front Percept. Sci. 3, 462, 1–8.

Brostoff, S. and Sasse, M.A. 2000. Are Passfaces more usable than passwords: A field trial investigation. In McDonald S., et al. (Eds.), People and Computers XIV-Usability or Else, Proceedings of HCI 2000, Springer, 405-424.

Bucci, W. 1985. Dual coding: A cognitive model for psychoanalytic research. Journal of the American Psychoanalytic Association, 33(3), 571-607.

Davis, D., Monrose, F. and Reiter, M. K. 2004. On user choice in graphical password schemes. Proceedings of the 13th Usenix Security Symposium. San Diego, CA.

Dhamija, R. and Perrig, A. 2000. Deja Vu: A User Study Using Images for Authentication. Proceedings of 9th USENIX Security Symposium

Gilhooly, K. 2005. Biometrics: Getting Back to Business. Computerworld. May 09.

Gokhale, M.A.S. and Waghmare, V. S. 2016. The shoulder surfing resistant graphical password authentication technique. Procedia Computer Science, 79, 490-498.

Gosselin, F. and Schyns, P. G. 2001. Bubbles: a new technique to reveal the use of visual information in recognition tasks, Vision Research 41, 2261–2271.

Hong, D. , Man, S. , Hawes, B. and Mathews, M. 2004. A password scheme strongly resistant to spyware. Proceedings of International conference on security and management. Las Vergas, NV.

Jansen W. 2004. Authenticating Mobile Device Users Through Image Selection. Data Security.

Jermyn, I. , Mayer, A. , Monrose, F., Reiter, M. K. and Rubin, A.D. 1999 The Design and Analysis of Graphical Passwords. Proceedings of the 8th USENIX Security Symposium.

Kirkpatrick, E. A. 1894. An experimental study of memory. Psychological Review, 1(6), 602.

Kotadia, M. 2005. Microsoft: Write down your passwords. ZDNet Australia. May 23.

Madigan, S. 2014. Picture memory. Imagery, memory and cognition, 65-89.

Man, S. , Hong, D. and Mathews, M. 2003. A shouldersurfing resistant graphical password scheme. Proceedings of International conference on security and management, Las Vegas, NV.

Mandler, J.M. and Ritchey, G.H. 1977. Long-term memory for pictures. Journal of Experimental Psychology: Human Learning and Memory, 3, 386-396

Mihajlov, M., Jerman-Blazič, B. and Ilievski, M. 2011. ImagePass-Designing graphical authentication for security. In Next Generation Web Services Practices (NWeSP), 2011 7th International Conference on (262-267). IEEE.

Miyachi, T., Takahashi, K., Hasegawa, M., Tanaka, Y. and Kato, S. 2010. A study on memorability and shoulder-surfing robustness of graphical password using DWT-based image blending. In Picture Coding Symposium (PCS), 2010 (134-137). IEEE.

Morris, R. and Thompson, K. 1979. Password security: A case study. Communications of the ACM, 22, 594-597.Norman, D.A. (1988). The Design of Everyday Things. Basic Books, New York

Norman, D.A., 1988. The Design of Everyday Things. Basic Books, New York.

Oliva, A., Torralba, A. and Schyns, P. G. 2006. Hybrid images. In ACM Transactions on Graphics (TOG) (Vol. 25, No. 3, 527-532). ACM.

Oliva, A. 2013. The art of hybrid images: Two for the view of one. Art and Perception, 1(1-2), 65-74.

Paivio, A., Rogers, T. B. and Smythe, P. C. 1968. Why are pictures easier to recall than words?. Psychonomic Science, 11(4), 137-138.

Perrig, A. and Song, D. 1999. Hash Visualization: A New Technique to Improve Real-World Security. Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce.

Shepard, R. N. 1967. Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior, 6, 156-163.

Sobrado, L. and Birget, J.C. 2002. Graphical passwords. The Rutgers Scholar An Electronic Bulletin for Undergraduate Research, 4.

Sowden, P. T. and Schyns, P. G. 2006. Channel surfing in the visual brain, Trends Cogn. Sci. 10, 538–545.

Suo, X. and Zhu, Y. and Owen, G. 2005. Graphical Passwords: A Survey. Proceedings of the 21st Annual Computer Security Applications Conference, 463-472.

Suo, X. 2006. A design and analysis of graphical password.

Syukri, A. F. , Okamoto, E. and Mambo, M. 1998 A User Identification System Using Signature Written with Mouse. Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 403-441.

Takahashi, K., Hasegawa, M., Tanaka, Y. and Kato, S. 2011. A structural similarity assessment for generating hybrid images. In Signals, Systems and Computers (ASILOMAR), 2011 Conference Record of the Forty Fifth Asilomar Conference on (240-243). IEEE.

Thorpe, J. and Oorschot, P. C. v 2004. Graphical Dictionaries and the Memorable Space of Graphical Passwords. Proceedings of the 13th USENIX Security Symposium. San Deigo, USA.

Tulving, E. and Watkins, M. J. 1973. Continuity between recall and recognition. The American Journal of Psychology, 739-748.

Valentine T. 1998. An evaluation of the Passface personal authentication system. Technical Report, Goldsmiths College, University of London.

Valentine, T. 1999. Memory for Passfaces after a Long Delay. Technical Report, Goldsmiths College, University of London.

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. and Memon, N. 2005. Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security (1-12). ACM

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. and Memon, N. 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human Computer Studies.

ÖZGEÇMİŞ

Adı Soyadı : Başak BİLGİ

Doğum Yeri : Ankara

Doğum Tarihi : 24.12.1983

Medeni Hali : Bekâr

Yabancı Dili : İngilizce, Almanca

Eğitim Durumu

Lise : Yıldırım Beyazıt Anadolu Lisesi (1999 – 2001)

Lisans : Ankara Üniversitesi Bilgisayar Mühendisliği (2009 – 2013)

Yüksek Lisans : Ankara Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı (Eylül 2013 – Haziran 2018)

Çalıştığı Kurumlar

Uzman Yazılım Mühendisi, CS Enformasyon Teknolojileri Ltd. Şti. 2013 –