GRAFİK TABANLI ŞİFRELERİN GÜVENLİK ANALİZİ İÇİN BİR YAKLAŞIM

Ahmet Emir DİRİK[*]

Özet: Grafik tabanlı şifreler, alfanümerik şifrelerden farklı olarak sistem ekranında görüntülenen bir imge üzerindeki bazı bölgelerin şifre olarak seçilmesi prensibine dayanmaktadır. Alfanümerik tabanlı şifrelere ait alfabe seti yaklaşık 70 karakterden oluşurken, grafik tabanlı şifrelerde alfabe boyutu kullanılan imgenin çözünürlüğüne bağlı olarak 1000 veya daha fazla olabilir. Bu da sistem güvenliğini önemli ölçüde arttırmaktadır. Bununla birlikte her yüksek çözünürlüklü imge yüksek entropiye sahip olmayabilir. Grafik şifrelerin alfanümerik şifrelere oranla daha güvenli olduğunu söyleyebilmek için kullanılan imgeye bağlı olarak grafik şifre entropisinin hesaplanması gerekmektedir. Bu çalışmada grafik şifrelerin güvenlik analizinde kullanılmak üzere bir grafik şifre entropi kestirim algoritması geliştirilmiştir. Geliştirilen algoritma grafik tabanlı şifrelemede kullanılan çeşitli imgeler üzerinde denenmiştir. Elde edilen sonuçlar önerilen algoritmanın grafik şifreleme sistemlerinde kullanılabileceğini göstermiştir.

Anahtar Kelimeler: Grafik tabanlı şifreler, entropi, focus of attention (FOA), güvenlik.

A Novel Approach for Security Analysis of Graphical Passwords

Abstract: Graphical passwords are different from classic alphanumeric based passwords such that graphical passwords are based on clicking some pixels on a system screen for system entry. The alphabet set of the alphanumeric passwords consists of nearly 70 alphanumeric characters whereas the alphabet size of graphical passwords would be more than 1000 depending on the resolution of the image used for graphical password. Thus using graphical passwords instead of alphanumeric ones would increase the security of the authentication systems. However, some images used for graphical passwords may not have high entropies. In order to say that the graphical passwords are better than the alphanumeric ones there should be a tool that computes or estimates the entropy of the graphical passwords. In this study an entropy estimation algorithm for graphical passwords is proposed to be used in security analysis of graphical passwords. The proposed algorithm is tested on several password images. The numerical result shows that the proposed entropy estimation algorithm can be used successfully in graphical password based authentication systems.

Keywords: Graphical passwords, entropy, focus of attention (FOA), security.

1. GİRİŞ

Günümüzde kullanıcı tanıma ve doğrulama sistemlerinde kullanılan şifreler genellikle alfanümerik tabanlıdır. Bu tip şifreler belli bir karakter setinden seçilmiş şifre dizisinin belli bir sıra ile sisteme girilmesi prensibine dayanmaktadır. Kullanıcı tanıma sistemlerinde alfanümerik şifrelere alternatif olarak biometrik veriler, parmak izi, retina taraması, ses tanıma, manyetik ve akıllı kart uygulamaları gibi bir çok farklı teknik de kullanılmaktadır (Uludag ve diğ. 2004). Alfanümerik şifrelere alternatif olarak önerilen her bir tekniğin kendine göre çeşitli avantaj ve dezavantajları bulunmaktadır. Örneğin biometrik tabanlı sistemler kişiye özel, çalınması veya unutulması imkansız şifreler sunarken biometrik veriyi yenilemek veya değiştirmek hiçbir zaman mümkün olmamaktadır. Ayrıca parmak izi tanıma sistemleri tamamen hatasız çalışmamakta, kullanıcılardan birinin parmağında herhangi bir cerrahi müdahale söz konusu olduğunda biometrik veri tamamen veya kısmen kaybolmaktadır. Manyetik kart ve pil tabanlı tanımlama sistemleri ise kullanıcının kim olduğunuzdan ziyade kimin o kartı taşıdığı ile ilgilenmektedir. Bu yüzden manyetik kart veya pilin kaybolma veya çalınma durumlarında çeşitli güvenlik problemleri doğabilmektedir. Bu problem her bir karta ait bir kişisel kimlik numarası (**PIN**: **P**ersonal **I**dentification **N**umber) ve şifrenin atanması ile çözülmeye çalışılmakta ancak bu da sistem maliyetlerini önemli ölçüde arttırmaktadır.

[*] Uludağ Üniversitesi, Mühendislik-Mimarlık Fakültesi, Elektronik Mühendisliği Bölümü, 16059, Görükle, Bursa.

Kullanıcı tanıma sistemlerindeki güvenlik problemi kullanılan şifrelerin alfabe setinin genişletilmesi ve/veya şifredeki basamak sayısının arttırılması ile çözülebilir. Ayrıca güvenliği arttırmak için belirli aralıklarla kullanıcılardan şifrelerini değiştirmeleri, şifrelerinde sadece rakam veya harf kullanmamaları, hatta şifre girişlerinde klavye yerine ekran üzerinde beliren sanal klavyelere fare veya kalem ile giriş yapmaları istenebilir. Bütün bu işlemler şifre oluşturma sürecini ve şifrenin kullanımını karmaşıklaştırarak şifre sahibi dışında kötü niyetli kişilerin sisteme girişlerini zorlaştırmaktadır. Bununla beraber güvenlik gerekçesi ile kullanıcı tanıma sistemlerinin daha karmaşık hale getirilmesi sistem kullanımını ve karmaşık şifrelerin hatırlanmasını zorlaştırılmaktadır. Hem yüksek güvenliğe sahip hem de kolay kullanılabilir bir kullanıcı tanıma sistemi tasarımı güvenlik sistemleri için önemli ve güncel bir problemdir (Jain 2000).

Grafik tabanlı şifreler kolay kullanımı ve alfanümerik şifrelere oranla daha güvenilir olması nedeni ile klasik şifreleme yöntemlerine bir alternatif olarak ortaya çıkmıştır. Grafik tabanlı şifre sistemleri, insanların görsel verileri yazı ve sayılara göre daha iyi hatırladığı hipotezine dayanmaktadır. Böylece kullanıcıların hatırlama kolaylığından dolayı zayıf ve kolay kırılabilen şifre oluşturma olasılıkları azalmaktadır (Jermyn 1999). Grafik tabanlı şifre sistemleri *tanıma* veya *hatırlamaya* dayalı olarak iki farklı şekilde geliştirilmektedir. Tanıma tabanlı sistemlerde kullanıcıların büyük bir imge seti içerisinden daha önce şifre olarak belirledikleri bir imgeyi tanıyıp seçmesi gerekmektedir. Sıralı hatırlamaya dayalı grafik tabanlı şifre sistemlerinde ise kullanıcılardan belirli bir imge üzerinde önceden seçilmiş noktaların sıra ile tıklanması istenmektedir. Bu tip sistemlerde kullanıcıya sunulan imge yardımı ile mevcut şifrenin hatırlanması kolaylaşmaktadır. Çünkü, grafik şifre mevcut imge içerisindeki bazı noktaların tıklanması ile oluşmakta, bu da kullanıcıların kendi oluşturdukları şifreleri daha kolay hatırlamalarını sağlamaktadır. Alfanümerik şifrelerde bunun gibi bir hatırlatıcı unsur bulunmamakta, bundan dolayı kullanıcılar kolay hatırlayabildikleri isim, tarih, yer, vb. bilgileri şifre seçiminde kullanmaktadırlar. Bu da alfanümerik şifrelerin kötü niyetli kişiler tarafından kırılmasını veya tahmin edilmesini kolaylaştırmaktadır.

Hatırlamaya dayalı ilk grafik tabanlı şifre sistemi 1996 yılında G. Blonder tarafından önerilmiştir (Blonder, 1996). Bu sistemde kullanıcı, şifresini ekranda görüntülenen bir imge üzerinde belirli noktalara tıklayarak oluşturmaktadır. Kullanıcının sistem tarafından tanınması için imge üzerinde önceden şifre olarak belirlenen bölgeleri veya yakın çevresini şifredeki sıra ile kullanıcı ekranı üzerinden tıklaması gerekmektedir. Bu sistemde birden fazla imge kullanılmamakta bunun yerine tek bir imge üzerinde belirli noktaların işaretlenmesi ile sisteme giriş yapılmaktadır. Boroditsky (2002) bu uygulamayı daha da basitleştirerek kullanıcıların tıklayabileceği bölgeleri imge üzerinde kalın çizgiler ile bir birinden ayırmış ve tüm imgeyi bir ızgara üzerine oturtarak kullanım kolaylığı sağlamıştır. Bu sistemin dezavantajlarından birisi imgenin kalın ızgara çizgileri ile bölünmesinden dolayı şifre alfabe setinin oldukça küçük olması ve bundan dolayı şifre uzunluğunun artmasıdır (örneğin her şifre için 12 tıklama). Sistemin bir diğer dezavantajı ise kullanıcıların kendi istedikleri imgeleri sisteme yükleyememeleridir.

Bu çalışmada kullanılan grafik şifre sistemi, hatırlamaya dayalı Wiedenbeck ve diğ. (2005) geliştirdiği *PassPoints* uygulamasıdır. PassPoints sisteminde kullanıcı şifre olarak kullanmak istediği her hangi bir imgeyi sisteme yükleyebilmekte ve hiç bir kısıtlama olmaksızın imge üzerindeki her hangi bir detayı şifre olarak seçebilmektedir. Bu yönü ile Wiedenbeck ve arkadaşlarının geliştirdiği bu sistem Boroditsky'nin önerdiği sistemdeki uzun şifre seçimi ve ızgara çizgileri altında kalan detayların şifre olarak seçilememesi gibi sorunlara alternatif bir çözüm getirmektedir. PassPoints uygulamasında kullanıcının seçtiği imge aynı zamanda hatırlatıcı bir görev görmekte, böylece kullanıcıların şifrelerini hatırlaması için herhangi bir yere not düşmesi gerekmemektedir. Ancak bu sistemde imge üzerindeki her nokta potansiyel olarak şifre seçiminde kullanılmaya aday olsa da, yüksek boyutlara sahip olan imgelerin düşük boyutlara sahip imgelere göre her zaman daha güvenli olduğu söylenemez. Örneğin çok ayrıntıya sahip olmayan bir imge, boyutu büyük de olsa, boyutu küçük fakat yüksek miktarda ayrıntı içeren karmaşık bir imgeye oranla şifre seçimi için daha az güvenilir olabilir.

Bu makalede önerilen metot yardımı ile PassPoints gibi sistemlerde kullanıcıların şifre için seçtiği imgelerin güvenlik analizi yapılabilmekte, böylece kullanıcıların seçtiği imgelerin grafik tabanlı şifre sistemlerinde kullanılıp kullanılamayacağı hakkında nicel bir değer üretilebilmektedir. Bu sayede grafik tabanlı kullanıcı tanıma sistemlerinin ve kullanıcıların güvenliği arttırılarak, zayıf ve kolay kırılabilecek grafik şifrelerin oluşturulması engellenebilecektir. Grafik şifrelerin güvenlik analizi literatürde genellikle alfabe boyutunun büyüklüğü ile değerlendirilmekte ve PassPoints gibi sistemlerde kullanılan şifre imgelerinin içerikleri kullanıcı ve sistem güvenliği açısından hesaba katılmamaktadır. Bundan dolayı bu çalışma PassPoints gibi hatırlamaya dayalı şifre sistemlerinin güvenlik analizinde literatürde bir ilk teşkil etmektedir.

2. GRAFİK TABANLI ŞİFRELER

Bu çalışmada önerilen grafik şifreler için entropi analiz algoritması PassPoints sisteminde denenmiştir. PassPoints sisteminde kullanıcılar şifre seçimini kendi seçtikleri bir imge üzerinde hatırlayabilecekleri noktaları belirleyerek yapmaktadırlar. Şekil 1'de PassPoint sistemine ait şifre toplama ekranı görülmektedir. Şekildeki kutular kullanıcının seçtiği şifre pozisyonlarını göstermektedir.

Şekil 1:
Grafik tabanlı şifre toplama yazılım ekranı.

Grafik şifre seçim süreci ilk olarak öğrenme fazı ile başlamaktadır. Bu süreçte kullanıcılar imge üzerinde N adet bölgeyi (Bu çalışma için N=5) 10-15 piksellik bir tolerans ile belli bir sıra ile seçerler. Şifrenin onaylanması için sistem kullanıcıdan kendi şifresini tekrar girmesini ister. Eğer kullanıcı arka arkaya aynı bölgeleri belli bir tolerans içerisinde tıklayabiliyorsa sistem kullanıcı ismi ile seçilen şifreyi ilişkilendirerek mevcut pozisyonların kuantalanmış halinin "hash" değerini kayıt eder (Tsudik 1992). Daha sonra kullanıcı sisteme girmek istediğinde öncelikle kendi ismini veya kısa adını klavyeden girer. Sistem klavyeden girilmiş kullanıcı adı ile ilişkilendirilmiş imgeyi ve kullanıcı şifresinin "hash" değerini hafızaya yükler. Kullanıcı sisteme girebilmek için ekranda beliren ve önceden kendisinin belirlemiş olduğu imgenin üzerinde şifresini oluşturan bölgeleri sırası ile tıklar. Eğer doğru noktaları doğru sıra ile tıkladıysa (tıkladığı imge pozisyonlarının hash değerleri kayıtlı değerler ile uyuşuyorsa) sisteme girebilir (Birget ve diğ. 2003). Eğer kullanıcı doğru noktaları tıklayamaz ise sistem kullanıcıdan şifre pozisyonlarını tekrar tıklamasını ister. Böyle bir sistemde grafik şifreyi oluşturan alfabe boyutu kullanılan imgenin boyutu ve tıklama toleransı ile belirlenmektedir. Tıklama toleransının arttırılması alfabe boyutunun azalmasına yol açmaktadır. 10x10 pikselik bir kare alanın tıklama tolerans bölgesini oluşturduğu düşünülürse, 640x480 boyutlarında bir imge 3072 adet farklı bölgeden oluşur ve böyle bir imgenin sahip olduğu grafik şifre alfabe boyutu 3072 olmaktadır. Bu değer alfa-nümerik tabanlı bir şifre için 60 civarındadır. Eğer söz konusu grafik tabanlı şifre en az 5 tıklama bölgesinden oluşuyor ise seçilebilen bir birinden farklı şifrelerin sayısı $3072^5 = 2{,}7\times10^{17}$ olacaktır. Böyle bir güvenlik değerini oluşturabilmek için 62 karakterden oluşan bir sete sahip alfa-nümerik şifre en az 10 basamaktan oluşmak zorundadır. Görüldüğü gibi grafik şifre kullanımı sayesinde karmaşık ve yüksek basamaklı alfa-nümerik şifrelerin sahip olduğu güvenlik düzeyine PassPoints gibi bir sistemde ekran üzerinde birkaç noktayı tıklayarak ulaşılabilmektedir. Bununla birlikte kullanıcıların seçtiği imgeler üzerinde belli bölge veya noktalar diğer bölgelere nazaran daha çok dikkat çekiyor olabilir (Findlay 1980, Senders 1997). Bundan dolayı kullanıcılar aynı veya benzer imgelerde sürekli aynı noktaları şifre olarak seçme eğiliminde olabilirler. Bu husus grafik şifrelerin entropisinin sanıldığının aksine en azından bazı imgeler için yeterince yüksek olamayabileceği anlamına gelir. Bu noktada grafik şifreler ile alfa-nümerik şifreleri birbiri ile karşılaştırmak için bir nicel değere ihtiyaç vardır. Bu değer ise grafik şifrelerin entropisinin kestirilmesi yardımı ile bulunabilir.

3. GRAFİK ŞİFRE ENTROPİSİNİN KESTİRİMİ

İnsanlar bir imgeye baktıklarında bazı bölgelere diğer alanlardan daha fazla dikkat etmektedirler. Örneğin grafik şifre seçiminde imge üzerindeki dikkat çekici, kontrastı yüksek bölgeler diğer alanlara göre daha çok tercih etmektedirler. İyi bir şifrenin kolay hatırlanabilir aynı zamanda da zor tahmin edilebilir

olması gerekmektedir. Bu da grafik şifre için kullanılacak imge seçiminin önemini arttırmaktadır. İyi ve kolay tahmin edilemeyen bir şifre için grafik şifrenin entropisinin yüksek olması gerekmektedir. Yüksek entropi şifrenin kırılmasının ve tahmin edilmesinin zorluğunun nicel bir ölçüsüdür.

Grafik şifrenin entropi kestiriminde ilk olarak imge üzerinde hangi bölgelerin daha çok dikkat çektiği tespit edilerek imgenin her bir noktası için önem olasılığını gösteren bir harita oluşturmak gerekir. Bu harita entropi hesabında şifre pozisyonlarının seçilme olasılıklarının belirlenmesinde kullanılacaktır. İmge üzerinde kullanıcıların hangi noktaları tıklayacaklarını kestirmek için ise şifre imgesi öncelikle bir "segmentasyon" işlemine tabi tutulur. Bu iş için literatürde önerilen temel segmentasyon algoritmaları incelenmiş ve "mean-shift" segmentasyon algoritmasının kullanılmasına karar verilmiştir (Comaniciu ve Meer 1999, Comaniciu ve Meer 2002). Mean-shift algoritması imge üzerindeki gereksiz detaylar ve zayıf renk dalgalanmalarını silerek önemli renkler ve ayrıtları korumaktadır. Bundan dolayı imge üzerindeki fazla enformasyonun silinmesi sürecinde önemli bir rol oynamaktadır. Segmentasyon işlemi ile imge segmentlere ayrıldıktan sonra her bir bölgenin "centroid" noktası (ağırlık merkezi) belirlenmekte ve bu noktalar imge üzerinde dikkat çekici olası şifre pozisyonları olarak kayıt edilmektedir (Şekil 2'de gösterilen noktalar). Segmentlerin centroid noktaları imge üzerindeki dikkat çekici noktalar olarak belirlendikten sonra birbirine çok yakın noktalar tek bir noktaya indirgenmektedir. Alanı görece büyük segmentlerin centroid noktaları ise düşük tıklanma olasılıklarından dolayı dikkate alınmamaktadır.

(a) (b)

Şekil 2:
Mean-shift segmantasyon algoritması yardımıyla belirlenen tahmini grafik şifre pozisyonları.

3.1. İmge üzerinde dikkat çekici bölgelerin (Focus of Attention) belirlenmesi

Olası şifre pozisyonları segmentasyon işlemi sonucunda belirlendikten sonra hangi noktanın daha dikkat çekici olduğunu belirleyen bir olasılık haritasının çıkarılması gerekmektedir. Bu konuda yapılan literatürdeki çalışmalar, insanın dikkatini belirleyen yüksek ve alçak seviye iki temel faktör olduğunu belirtmektedir. Yüksek seviye faktörler hafıza şablonları ile örtüşme ve hatırlamaya dayalıdır. Örneğin yüz kişilik bir salon içerisinde sadece bir kişiyi tanıyorsanız ve diğer kişiler size yabancı ise ister istemez tanıdığınız kişiye odaklanırsınız. Düşük seviye faktörler ise görüntü üzerindeki kontrast, biçim, boyut, renk, hareket, arka plan gibi imgenin kendisine ait bazı karakteristik özelliklere bağlıdır (Zhao ve diğ. 1996, Osberger ve Maeder 1998). Bu faktörler içinde insan dikkatini en çok çeken özelliklerden bir tanesi kontrasttır (Elias ve diğ. 1984, Yarbus 1967). Bir diğer dikkat çekici faktör ise şekil boyutlarıdır ancak aşırı büyük veya küçük boyutlardaki obje ve şekiller için dikkat çekicilik faktörü çok yüksek değildir. Bazı renkler, örneğin kırmızı renk diğer renklere göre insan dikkatini daha çok çekmektedir. Bunun dışında imgenin içeriği de insan dikkatini çeken bir faktör olarak ele alınabilir. Örneğin insanların içinde bulunduğu bir görüntü veya manzarada özellikle gözler, ağız ve eller diğer noktalara göre daha çok dikkat çekmektedir (Patrick 2004). Bir imge üzerinde hangi noktaların daha çok dikkat çekici olduğunu belirleyebilmek için yukarıda sayılan tüm faktörlerin bir arada değerlendirilmesi gerekmektedir. Bu uygulamada ise sadece belli başlı bazı dikkat çekici faktörler (kontrast, renk, ön plan) kullanılmıştır. Kullanılan algoritma genişlemeye müsait olduğundan istenildiği takdirde diğer faktörler de sisteme dahil edilebilir.

3.1.1. Karşıtlık

Mean-shift segmentasyon işlemi ile imge bölümlere ayrıldıktan sonra her bir segmentin diğer segmentlere oranla ne ölçüde insan dikkatini çektiği karşıtlık, renk ve arka plan gibi özniteliklere bağlı olarak belirlenmekte ve tüm bir imge için kullanıcıların dikkatinin nereye odaklandığını gösteren FoA (Focus of Attention) haritası oluşturulmaktadır. Karşıtlık insan dikkatini çeken en önemli düşük seviye faktörlerden birisi olduğundan bu uygulamada FoA haritasının oluşturulmasında birinci temel öznitelik olarak kullanılmıştır. Herhangi bir segmente ait karşıtlık özniteliği o segmentin parlaklık değeri ile diğer komşu segmentlerin renklerinin parlaklık değerlerinin farkı olarak aşağıdaki şekilde hesaplanmaktadır.

$$karsitlik(seg_i) = \frac{\sum_{k=1}^{N_i} \left| parlaklik(seg_i) - parlaklik(seg_k) \right|}{N_i} \tag{1}$$

Burada *parlaklık(seg$_i$)* değeri, "ee". segmentin gri seviyesini belirtmektedir. N_i değeri "ee" numaralı segmentin komşu segmentlerinin sayısını vermektedir. *parlaklik(seg$_k$)* ifadesi ile "ee" numaralı segmente komşu olan segmentlerin gri seviye değerleri belirtilmiştir.

3.1.2. Renk Farkı

FoA haritasını oluşturan ikinci öznitelik ise renk karşıtlığına göre hesaplanmaktadır. RGB haritası tüm renklerin üç kanal yardımı ile betimlenmesi esasına dayanmaktadır. Ancak imgedeki ana renklerin tespiti için RGB formatı yeterli olmamaktadır. HSV (Hue, Saturation, Value) uzayı ise bu amaç için daha uygun olduğundan her bir segmentin RGB değerleri HSV uzayına dönüştürülür. RGB bilgisi HSV formatına dönüştürüldükten sonra sadece hue değerine bakarak ilgili segmentin renk değeri hakkında bilgi edinilebilir.

$$renkfarki(seg_i) = \frac{\sum_{k=1}^{N_i} \left| hue(seg_i) - hue(seg_k) \right|}{N_i} \tag{2}$$

Dolayısı ile renk kontrastı hesaplanırken ilgili segmentin "hue" değeri ile komşu segmentlerin "hue" renk değerleri formül (2) de belirtilen şekilde karşılaştırılmaktadır.

3.1.3. Ön/arka alan

Bu öznitelik imge üzerindeki objeleri arka plandan ve fon görüntüsünden ayırmak amacı ile kullanılmaktadır. Bunun için segmentasyon işlemi ile birbirinden ayrılmış bölgelerin kenar uzunluklarının tüm imgenin kenar uzunluğuna oranı hesaplanarak segmentler için uzunluğa bağlı ön ve arka plan analizi yapılmıştır. Önalan özniteliği formül (3) teki gibi hesaplanmaktadır.

$$önalan(seg_i) = 1 - \min\left(\frac{çevre(seg_i)^{1,3}}{toplamçevre}, 1 \right) \tag{3}$$

Burada *çevre (seg$_i$)* ifadesi ile "ee" numaralı segmentin kenar uzunluğu belirtilmekte, *toplamçevre* değeri ise imgenin toplam kenar uzunluğunu vermektedir. Formülde belirtilen 1,3 "ee" ifadesi empirik olarak belirlenmiştir. Bir segmentin kenar uzunluğu büyüdükçe o segmente ait önalan öznitelik değeri formül 3'ten görüleceği gibi azalmaktadır.

Şekil 3:
Tahmini şifre pozisyonları ve FoA haritaları.
(Imgeler www.freefoto.com adresinden alınmıştır.)

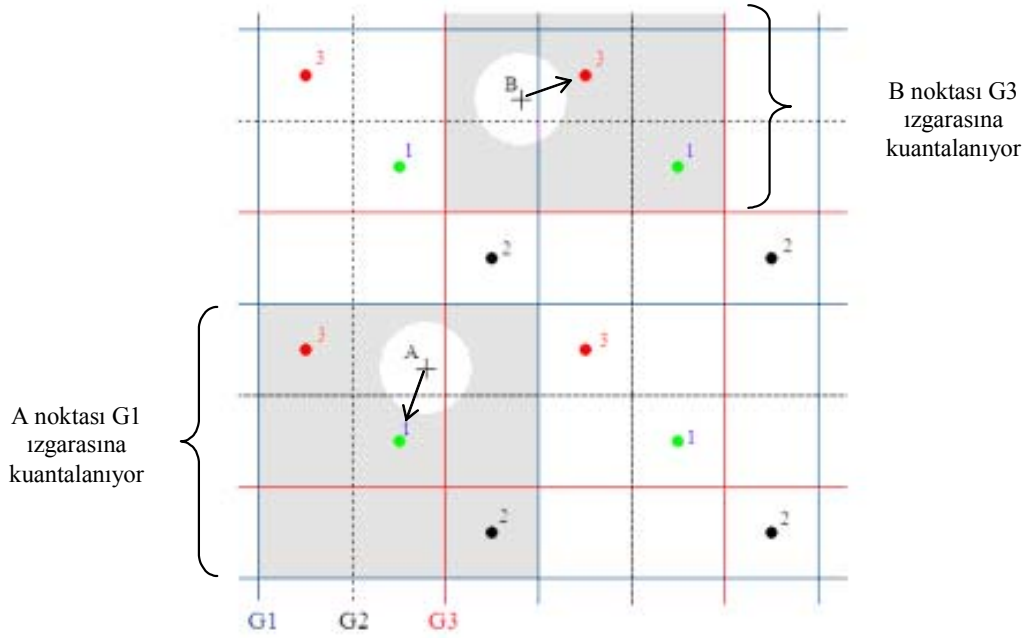
3.1.4. Özniteliklerin Birleştirilmesi

Yukarıda açıklanmış olan 3 temel öznitelik imge üzerindeki her bir segment için ayrı ayrı hesaplandıktan sonra 0 ile 1 arasına normalize edilir ve (4) numaralı formül ile birleştirilerek her bir segment ait dikkat çekme (FOA) değeri hesaplanır.

$$FOA(seg_i) = \sum_{k=1}^{3} W_k \cdot öznitelik_k(seg_i) \tag{4}$$

Formülde (4) te belirtilen W_k değeri her bir özniteliğe verilmiş olan ağırlık değeridir. Örneğin karşıtlık bilgisi diğer özniteliklerden daha önemli olduğundan karşıtlığa ait olan ağırlık katsayısı diğer niteliklere göre daha büyük seçilmiştir. Formül 4'te her ne kadar 3 tane öznitelik görülmekteyse de FOA haritasını oluşturmak için kullanılacak öznitelik sayısında bir sınırlama bulunmamaktadır. Şekil 3'te formül (4) ile hesaplanmış farklı imgelere ait FOA haritaları ve önemli segmentlerin cetroid noktaları görülmektedir. FoA haritasında aydınlık alanlar dikkat çekici bölgelerin tahmini yerlerini, karanlık alanlar ise daha az dikkat çeken yerleri belirtmektedir.

Segmentlerin centroid pozisyonları ve her segmente ait FOA bilgisi hesaplandıktan sonra imgeye ait grafik şifrenin entropisi hesaplanabilir. Ancak bu işlemden önce imge üzerindeki tahmini şifre pozisyonlarının kuantalanıp kodlanması gerekmektedir. PassPoint grafik tabanlı şifreleme sisteminde kullanıcı şifre olarak kendi yüklediği imge üzerindeki her hangi bir noktayı şifre olarak atayabilir. Ancak kullanıcılar fare veya kalem (stylus) ile tekrar tekrar aynı noktayı tıklamak istediklerinde her zaman ilk belirledikleri noktayı değil o noktaya yakın bölgeleri tıklayabilmektedirler. Bu da bir hata değeri oluşturmaktadır.



Şekil 4:
Grafik şifre pozisyonlarının kuantalama ve kodlanması.

Herhangi bir 4 basamaklı bir kullanıcı şifresinin (103,235)-(145,167)-(10,459)-(54,132) şeklinde imge üzerindeki 4 adet nokta olduğunu varsayalım. Bu noktalar sisteme kayıt edilirken hata toleransı dikkate alınarak bir satranç tahtasındaki kare kodlarını andıran bir kodlama tekniği ile kuantalanırlar (Birget 2003). Kodlama işlemi bittikten sonra her bir kod güvenli ve tek yönlü "hash" fonksiyonundan geçirilerek sisteme açık olarak kayıt edilir. Şifre pozisyonları kuantalandıktan sonra "hash" değerleri ile saklandığından sistemdeki kayıtlara bakan kötü niyetli birisi kullanıcının şifresini elde edemeyecektir. Kullanıcı şifreleri imge üzerindeki ızgara şeklindeki sanal karelere bağlı olarak kuantalandığından imgeye ait tahmini alfabe boyutunun hesaplanmasında da kuantalama işleminden yararlanılmalıdır. Bu yüzden segmentasyon işlemi ile tespit edilen tahmini şifre pozisyonları sahip oldukları FOA değerleri ile birlikte Birget (2003)'in önerdiği şekilde kuantalanırlar. Şekil 4'te kuantalama işleminin nasıl yapıldığı görülmektedir.

Şekil 4'te G1, G2 ve G3 ile gösterilmiş 3 farklı ızgara üzerinde + işaretli noktalar ve etrafındaki çemberler kullanıcının şifre olarak seçtiği yeri ve hata tolerans bölgesini göstermektedir. Resimdeki numaralar ise ızgara içindeki karelerin kuantalama merkezlerini göstermektedir. A ve B noktalarını tıklayan kullanıcının şifresi A ve B noktalarının piksel değerleri yerine G1, G2 ve G3 şeklinde adlandırılan 3 farklı ızgaranın belirlediği karelerin kodları ile kayıt edilir. Örneğin A noktası ve etrafındaki tolerans çemberi G3 ve G2 ızgaralarını kestiği için A noktası mavi renkli 1 numaralı ızgaraya ait karenin merkezine kuantalanır. B noktası ise 1 ve 2 nolu ızgaraları kestiği için 3 nolu kırmızı renkli ızgaranın merkezine kuantalanır (Birget 2003). Tahmini şifre pozisyonları yukarıda açıklandığı gibi kuantalandıktan sonra belli kuanta merkezlerine birden fazla tahmini pozisyon taşınması durumunda kuanta merkezinin FOA değeri oraya taşınan her bir tahmini şifre pozisyonunun FOA değerlerinin toplamı şeklinde hesaplanmaktadır. Pozisyonların kuantalanması ile birlikte imgenin tahmini alfabe boyutu ve her bir alfabeyi oluşturan pozisyonun tıklanma olasılığı belirlenerek imgeye ait grafik şifrenin entropi değeri belirlenebilir.

4. DENEYSEL SONUÇLAR

Bu çalışmada önerilen grafik şifrelerin entropi kestirimi algoritması özel seçilmiş iki farklı imge üzerinde denenerek bu imgelerin güvenlik analizi gerçekleştirilmiştir. Bu imgelerden ilki basit ve şifre uygulamaları için kötü kabul edilebilecek *kuşlar* imgesinden (şekil 5) diğeri ise ilk imgeye göre daha güvenli görünen ve daha kompleks olan *sokak* (şekil 6) imgesinden oluşmaktadır.

(a) Tahmini şifre pozisyonları (kırmızı noktalar) (b) Dikkat çekici bölgeler (FOA haritası)

Şekil 5:
Kuşlar imgesine ait tahmini şifre bölgeleri ve o bölgelerin dikkat çekicilik değerleri

Kuşlar imgesinin güvenlik analizi için yukarıda anlatıldığı üzere ilk olarak imge mean-shift segmentasyon algoritması ile segmentlere ayrılmış daha sonra her bir segmentin centroid noktalarına bağlı olarak tahmini şifre pozisyonları belirlenmiştir (Şekil 5a'da görülen kırmızı noktalar). Daha sonra her bir segmentin FOA değeri hesaplanarak imge üzerindeki en çok dikkat çeken yerler belirlenmiştir. Kuşlar imgesine ait FOA haritası Şekil 5b'de görülmektedir. Şekil 5b'de kuşlar imgesinde dikkati daha fazla çeken yerler beyaz, az çeken yerler ise gri ve siyah renkler ile gösterilmiştir. Ayrıca aynı şekil üzerinde segmentlerin sınırları da gösterilmiştir. Şekil 5'ten görüldüğü gibi imge üzerindeki kuşlar kontrastı ve ön planda oluşu nedeni ile en çok dikkati çeken bölgeler olarak belirlenmiştir. Son aşamada FoA haritası belirlenip tahmini şifre pozisyonları kuantalanarak kuşlar imgesinin entropisi 5.20 bit olarak hesaplanmıştır (Çizelge 1).

(a) Tahmini şifre pozisyonları (kırmızı noktalar) b) Dikkat çekici bölgeler (FOA haritası)

Şekil 6:
Sokak imgesi için tahmini şifre pozisyonları

Bu çalışmada önerilen entropi kestirim algoritması *kuşlar* imgesine göre daha karmaşık olan *sokak* isimli imge üzerinde de denenmiştir. Sokak imgesi için hesaplanmış tahmini şifre pozisyonları Şekil 6'da verilmiştir. Tahmini pozisyonlar ve FOA haritası hesaplanıp, şifre pozisyonları kuantalandıktan sonra sokak imgesinin entropisi 7.25 bit olarak bulunmuştur (Çizelge 1). Şekil 7'deki kırmızı noktalar algoritmanın belirlediği tahmini şifre pozisyonlarıdır. Sokak imgesi arka planındaki ağaç ve duvar detayları için algoritma herhangi bir pozisyon tahminde bulunulmazken ön plandaki insan figürleri en çok hit alan yerler olarak görünmektedir. Ayrıca sokak imgesi ile kuşlar imgesinin boyutları aynı olmasına rağmen, sokak imgesine ait alfabe boyutu 194 kuşlar imgesine ait alfabe boyutu 43 olarak hesaplanmıştır. Alfabe boyutu

için 43 değeri yetersiz kalırken alfabe boyutunun 194 olması güvenli bir şifrenin oluşturulması için yeterli bir değerdir. Sokak imgesinde 5 basamaklı bir grafik şifre için 194^5 = 274,8 milyar farklı şifre seçmek mümkün iken bu değer kuşlar imgesinde 43^5 = 147 milyon'dur. Çizelge 1'den de görüleceği gibi sokak imgesi grafik şifreleme sistemlerinde kullanılmak için kuşlar imgesine oranla da uygundur.

Çizelge 1:
İmgelere ait tahmini grafik şifre entropileri

	Kuşlar imgesi	Sokak imgesi
İmge üzerindeki tıklanabilecek birbirinden farklı kuantalanmış pozisyonların sayısı	210	210
Grafik şifreye ait tahmini alfabe boyutu	43	194
Grafik şifrenin entropisi (bit)	5.20	7.25

5. TARTIŞMA VE SONUÇ

Güncel bir teknoloji olan grafik tabanlı şifreler alfanümerik şifrelere göre bir çok avantajlara sahiptir. Grafik şifreler insanların görüntüleri sayı ve rakamlara göre daha iyi hatırladıkları hipotezine dayanmaktadır. Ayrıca grafik şifrelerin karakter tabanlı şifrelere oranla daha güvenli olduğu söylenebilir. Grafik şifreler kullanıcıların bir resim üzerindeki noktaları belli bir sıra ile tıklamaları ile oluşturulduğundan yüksek çözünürlüklü imgeler daha güvenilir şifrelerin oluşturulmasına imkan sağlamaktadır. Ancak grafik şifrenin güvenilir ve zor kırılabilir olduğunu söylemek için kullanılan imgenin içeriğinin bilinmesi gerekir. Bu noktada hangi tip imgelerin grafik şifreler için uygun olacağı sorusu sistem güvenliği açısından büyük önem taşımaktadır.

Bu çalışmada grafik tabanlı şifreleme sistemlerinde kullanılan imgelerin güvenlik analizi için yeni bir metot önerilmiş ve önerilen metot çeşitli imgelerin güvenlik analizinde başarı ile denenmiştir. Elde edilen nümerik sonuçlar bu çalışmada önerilen metodun grafik şifrelerin güvenlik analizinde kullanılabileceğini göstermektedir. Grafik şifrelerin güvenlik analizi imgenin içeriği dikkate alınarak gerçekleştirilmektedir. Kullanıcıların imge üzerinde şifre olarak seçebilecekleri yerler FoA (Focus of Attention) bölgelerinin tespiti yardımı ile belirlenmiş bu sayede imgelerin sahip oldukları tahmini grafik şifreye ait alfabe boyutu kestirilebilmiştir. Bu çalışmada önerilen grafik şifrelerin entropi kestirim algoritması ile grafik şifrelerin karakter tabanlı şifreler ile güvenlik açısından karşılaştırılması da mümkün olabilmiştir.

Bu çalışma imge tabanlı (PassPoints, vs.) grafik şifrelerin entropi kestirimi ve analizinde bir ilk teşkil etmektedir. Bununla birlikte kullanıcıların şifre seçim yaklaşımlarının doğru olarak modellenebilmesi için farklı içeriğe sahip çok sayıda imge için yüzlerce kullanıcıdan grafik şifre bilgilerinin toplanması ve bu bilgilere göre önerilen metodolojinin güncellenmesi gerekmektedir. Böylece daha doğru bir entropi kestirim modeli oluşturulabilir. Gelecek çalışmalarda kullanıcılardan elde edilen bilgiler ile önerilen metodolojinin karşılaştırılması ve gerekiyorsa gerekli güncellemelerin yapılması düşünülmektedir.

Ayrıca makalede önerilen metodoloji ile grafik şifreler için mümkün olmayan sözlük tabanlı şifre saldırıları mümkün olmaktadır. Şifre modeli ile kestirilen tahmini alfabe üzerinden FOA haritası da kullanılarak akıllı bir şifre saldırı algoritması geliştirilebilir. Böyle bir saldırının boyutları ve karşı önlemlerin geliştirilmesi gelecek çalışmaların da içeriğini oluşturacaktır.

6. TEŞEKKÜR

Bu çalışmaya verdiği desteklerinden dolayı Nasir Memon ve Alex Broditsky'e teşekkür ederim.

7. KAYNAKLAR

1. Birget, J. C., Hong, D. and Memon, N. (2003) Robust discretization with application to graphical passwords, *Cryptology ePrint Archive*.
2. Blonder, G. (1996) Graphical passwords, *United States Patent*, (5559961).
3. Boroditsky, M. (2002) *Passlogix password schemes*, http://www.passlogix.com.
4. Comaniciu, D. and Meer, P. (1999) Mean shift analysis and applications, *7th International Conference on Computer Vision*, pages 1197-1203.

5. Comaniciu, D. and Meer, P. (2002). Mean shift: A robust approach toward feature space analysis, *IEEE Transactions on pattern analysis and machine intelligence*, 24(5):603-619.
6. Elias, G., Sherwin, G. and Wise, J. (1984) Eye movements while viewing ntsc format television, *SMPTE Psychophysics*, Subcommittee white paper, Mar.
7. Findlay, J. (1980) The visual stimulus for saccadic eye movement in human observers, *Perception*, (9):7-21, Sept.
8. Jain, A., Hong, L. and Pankanti (2000) S. Biometric identification. *CACM 43*, pages 91-98.
9. Jermyn, I., Mayer A., Monrose, F., Reiter, MK., Rubin, AD. (1999) The design and analysis of graphical passwords, *8th Security Symposium,* Washington DC.
10. Osberger, W. and Maeder, A. J. (1998) Automatic identification of perceptually important regions in an image, *Proceedings of Fourteenth International Conference on Pattern Recognition*.
11. Patrick, A. S., Long, A. C. and Flinn, S. (2004) Hci and security systems, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 24-29. ACM.
12. Senders, J. (1997) Distribution of attention in static and dynamic scenes, *Proceedings SPIE* 3016, pages 186-194. SPIE, Feb.
13. Tsudik, G. (1992) Message Authentication with One-Way Hash Functions, *Proceedings of IEEE INFOCOM 1992*, May.
14. Uludag, U., Pankanti, S., Prabhakar, S. and A. K. Jain (2004) Biometric Cryptosystems: Issues and Challenges, *Proceedings of the IEEE*, *Special Issue on Enabling Security Technology for Digital Rights Management*, Vol. 92, No. 6, pp. 948-960.
15. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., Memon, N. (2005) PassPoints: Design and longitudinal evaluation of a graphical password system, *International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security)*, 63, 102-127.
16. Yarbus, A. (1967) Eye Movements and Vision, Plenum Press, New York, NY.
17. Zhao, J., Shimazu,Y., Ohta, K., Hayasaka, R. and Matsushita, Y. (1996) An outstandingness oriented image segmentation and its application. *ISSPA*, pages 45-48.