# Uygulamalarda Şifre Güvenliği İçin Yeni Bir Yaklaşım

Y. Sönmez, M. Karabatak ve E. Avcı

***Özet*** **— Günümüz bilgisayar teknolojisinde kullanılan programların çoğunda (masaüstü programlar, e-mail, web sayfaları vs.) kişiye ait bilgiler bulunmakta ve bu ortamlara girişte bu bilgilerin doğru kişiye sunulması için kullanıcı adı ve şifre kombinasyonuna dayalı güvenlik sistemleri kullanılmaktadır. Bu güvenlik sistemlerindeki kullanıcı adı ve şifreler sayısal veya karakter tabanlı olup klavye aracılığı ile girilmektedir. Kişiye ait bilgilere ulaşmaya çalışmak için yapılan saldırılar klavye dinleme donanım veya yazılımları ile yapılmaktadır. Klavye dinleme donanım veya yazılımları tuş vuruşlarını kaydederek saldırıyı yapan kişi/kişilere göndermekte ve kullanıcı adı ve şifreler çalınabilmektedir. Geliştirilmeye çalışılan sistemde şifrenin kişiye özgü olmasını sağlayan bir program yapılmaya çalışılmıştır. Kişiye özgü şifreden kasıt, kullanıcının şifre girişi esnasındaki klavye kullanım tarzını tespit ederek şifre güvenlik düzeyinin arttırılmasına yöneliktir. Bu sayede şifreler saldırı yapan kişi/kişilerin eline geçse dahi, şifrenin gerçek sahibi gibi aynı tarzda yazılamayacağından dolayı girilen şifre yanlış kabul edilecektir. Şifrelerin belirli tarzda yazılmasının tespiti bilgisayarlara duyusal anlama boyutu katmakta ve şifreyi kullanan kişi tarafından yazılıp yazılmadığı kontrolü sağlanmaktadır.**

***Anahtar Kelimeler***— **Güvenli şifre, Klavye dinleme sistemleri, Klavye kullanım tarzı.**

***Abstract***— **Many of the programs (Desktop Programs, e-mail, web sites, and etc.), which they have been used thanks to today's computer technology, keep personal information in themselves. In order to present right personal information to right people, a protection system, which is based on user names and password combination, is used. User names and passwords in this protection system, which are entered through a keyboard, are numerical and character based. Attacks, which are aimed to be able to access to exclusive information, are done through a keyboard monitoring system by using related hardware and software. It is likely to steal some of personal information such as user names and passwords by using various kinds of hardware and software tools which works based on keyboard monitoring system. In the program we aim to develop, the main goal is to ensure password security by making passwords private. The main aim of using the term 'Private Password' is to identify keyboard using style of each person, thus aiming at increasing password security level. Thanks to such a this kind of system, even if password are captured by people who attack to our computer systems, these passwords are regarded as wrong passwords or information since passwords cannot be written with the same style of passwords' real owners. The identification of passwords' writing style contributes to sensory analysis of computers, thus establishing control in computers by checking whether passwords are written by real owners of them or not.**

***Keywords***— **Secure Password, Keyboard Monitoring Systems, Keyboard Using Style.**

## I. GİRİŞ

TEKNOLOJİNİN hızla gelişmesi ve sayısal sistemlerin yoğun bir şekilde kullanılmasıyla bu sistemlerdeki veri güvenliği de büyük ölçüde önem kazanmıştır. Bilişim teknolojilerinde güvenliğin sağlanmasındaki temel amaç kullanıcıların bu teknolojileri kullanırken karşılaşabilecekleri tehdit ve tehlikelere karşı gerekli önlemlerin alınmasını sağlamaktır[1]. Kişilere ait bilgilerin veri olarak saklanması ise güvenlik sistemlerinden beklenen iki temel görev, veriyi ait olduğu kişilere sunmak ve yabancı kişilere veriyi kapatmaktır[2]. Bu veriler saklanırken ve kişilerin erişimine sunulurken, ait olduğu kişiye sunulması için kullanıcı adı ve şifre kombinasyonuna dayalı güvenlik sistemleri kullanılmaktadır. Bu tip güvenlik sistemleri bilgi temelli kimliklendirme olarak adlandırılır [3]. Bu çeşit güvenlik sistemlerinde kullanıcı adı ve şifreler bir veri tabanında tutulur. Kullanıcılar bilgilerini sisteme girdiklerinde veritabanında karşılaştırma yapılır. Karşılaştırma sonucu bilgiler aynı ise doğru kullanıcı olduğu anlaşılır ve söz konusu kullanıcının sisteme giriş yapmasına ve sistemde kendisine tanınan yetki dâhilindeki işlemleri gerçekleştirmesine izin verilir. Bu tip sistemlerin en önemli dezavantajlarından biri, kullanıcının şifre bilgisinin bir başkası tarafından elde edilmesinin klavye dinleme sitemleri sayesinde kolay oluşudur [4].

Şifre güvenliğini arttırmaya yönelik olarak; kullanıcı eğitimi, otomatik üretilmiş parolaların kullanımı, ardıl (reactive) parola denetimi ve öncül (proactive) parola denetimi gibi teknikler kullanılmaktadır [5]. Uzun yıllar, "insan-makine ara yüzünde" var olan güvenlik açıkları ise çoğunlukla göz önüne alınmamıştır. Bir "insan makine ara yüzü" olarak bilgisayar kullanırken en çok etkileşimde bulunulan donanımların başında gelen klavyeler, bilgisayar sistemlerinin en az değişen ve üzerinde en az durulan donanımlarından biridir [6]. Kullanıcıların klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları saldırı yapan kişi/kişilere gönderen keylogger olarak adlandırılan kötü amaçlı yazılımlar ile şifreler kolaylıkla çalınabilmektedir. Üstelik kötücül ve casus yazılımlara karşı hazırlanan paket programların (anti virüs) çoğu, klavye dinleme sistemlerini dikkate almadığı öne sürülmektedir [7]. Şifreler kişi/kişiler tarafından ele geçirildikten sonra ilgili sistemlere kötü amaçlı yazılımlar sayesinde rahatlıkla giriş yapılmaktadır. Dolayısıyla günümüz teknolojisinde henüz şifrelerin kişi/kişiler tarafından ele geçirilip kullanılmasına karşı yüzde

yüz güvenli bir yöntem geliştirildiğinden söz edilememektedir.

Şifre kullanımındaki diğer bir sorun da, genellikle birçok ortamda aynı şifrenin kullanılıyor olmasıdır. Kullanıcıların çoğu, farklı şifreler kullanıldığında bunu hatırlamanın çok zor olması nedeni ile aynı şifreyi birçok sistemdeki kullanmaktadır [8]. Bu nedenle şifresi ele geçirilen bir kullanıcının, şifresi ile erişim yaptığı tüm uygulamalara giriş için gerekli olan anahtar olan şifre doğrudan ele geçirilmiş olmaktadır. Bu da şifre güvenliğinin ne kadar önemli olduğunu açık bir şekilde ortaya koymaktadır.

Klavye dinleme yazılımı olarak bilinen ve keylogger olarak adlandırılan kötücül yazılımlara karşı alınan önlemler günümüzde yeterli seviyede değildir. Bu sebepten dolayı, kişilerin klavye kullanım tarzının tespit edilmesi ve güvenlik düzeyinin arttırılması amacı ile şifre girişleri için yeni bir yaklaşım sunulmuştur. Böylece şifreyi yazan kişinin doğru kişi olup olmadığının tespiti yapılmakta ve şifreler başka kişi/kişiler tarafından ele geçirilse dahi şifrenin gerçek sahibi tarafından girilip girilmediği belirlenmektedir. Dolayısıyla, uygulamalara kazandırılan bu boyut sayesinde, yabancı kişi/kişiler tarafından şifre doğru girilse dahi bu giriş sistem tarafından otomatik olarak ret edilecektir.

Geliştirilen bu özellik ile, istenmeyen kişi/kişilerin ellerine geçen şifrelerin kullanılmasında caydırıcılık özelliği de sağlanmaktadır. İstenmeyen kişiler tarafından doğru şifre girilmesine rağmen, sistem tarafından şifrenin yanlış olduğu iletilmektedir. Böylece şifreyi ele geçiren kişi doğru şifreyi girmediğini varsayarak aynı şifreyi tekrar denemeyecek ve sisteme giriş yapma ihtimali kalmayacaktır.

Literatürde, şifre güvenliğinin sağlanmasına yönelik farklı yöntemlere rastlanmaktadır. Bu çalışmada önerilen yöntem, biyometrik kimliklendirme yöntemlerine benzemekte ve sadece kişinin kendine özgü bir davranışının analiz edilerek şifre girişine uygulanmasını içermektedir. Biyometrik sistemler, fiziksel ve davranışsal olmak üzere iki guruba ayrılan özellikleri içermektedir. Davranışsal biyometrik sistemlerden olan el yazısı analizinde, daha önce kişinin yazdığı bir yazı ile yeni yazdığı yazılar çeşitli adli tıp uzmanları veya görüntü işleme teknikleri ile tespit edilmektedir [9]. Bu tespit, kişinin harfleri nasıl yazdığına bakıp karşılaştırmaktadır. Örneğin "j" veya "i" harflerini yazarken nokta bırakma, düz çizgi çizme şekilleri gibi kişiye özgü olan durumlar tespit edilmektedir. Önerilen bu sistemde de kişinin klavye kullanırken bir kelimeyi nasıl kodladığı bu kodlamayı yaparken tuşlara hangi hızda bastığı tespit edilip şifre güvenliğinde kullanılması analiz edilmiştir.

## II. YÖNTEM

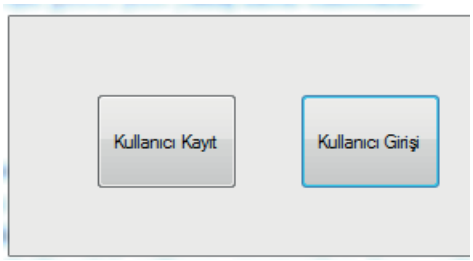
Bilgisayar veya uygulama programlarını kullanan her kişinin, farkında olsun olmasın klavye kullanırken kendine özgü geliştirdiği bir yazım tekniği olduğu yapılan gözlemlerle tespit edilmiştir. Bu gözlemler ile tespit edilen bu teknik kişinin klavye kullanırken yazım hızı ve kodlaması olarak ifade edilmiştir. Şifre bilgisi gibi bilgiler günlük yaşamda çok sık kullanıldığı için bu bilginin bilgisayar sistemlerine girilmesinde kişiye özgü bir tarz ortaya çıkmaktadır. Örneğin kişi "Fırat" kelimesini yazarken, tuşlara "Fı-rat", "F-ırat" veya "Fır-at" yazacak şekilde klavye kullanımı gerçekleştirmektedir. Bu kullanım tarzı şifre gibi aynı bilginin çok sık kullanılması ile daha belirgin hale gelmektedir. Çünkü bilgisayar kullanırken şifre ile giriş yapılan yazılımlarda genellikle aynı şifreler kullanılmakta ve bu şifreler sürekli kullanımdan dolayı sürekli aynı kodlama ve hızda girilmektedir.

Bu aşamada, kişinin klavye kullanım tarzının tespit edilmesi ile kişiye özgü şifre oluşturulması gerçekleştirilecektir. Bu nedenle, şifre ile giriş yapılan yazılımlara (mail, üyelik girişi, kredi kartı şifre girişi vs. gibi) giriş yapmak için kullanılan şifrenin doğru kişi tarafından girilip girilmediğinin kontrol edilmesi gerekmektedir. Bu prensibe dayanarak geliştirilen algoritma ile kişinin şifre girişi esnasındaki tuşlara basma hızı ve kodlama şekli tespit edilmekte ve şifrenin doğru olup olmadığının yanı sıra doğru kodlama ve hız ile girilip girilmediği de kontrol edilmektedir.

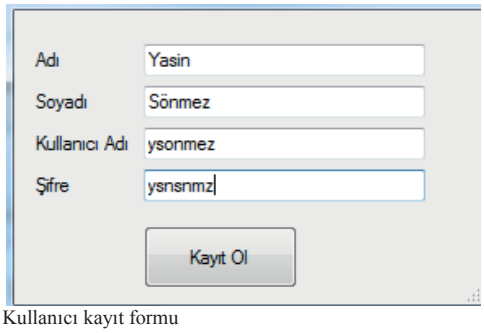
Örneğin kullanıcı, şifre bilgisi olarak “1234” bilgisini yazarken hangi hızla yazdığı veya “12” yazdıktan sonra “2” yi silip tekrar “234” yazarak şifreyi tamamladığında bu giriş tarzı da takip edilerek şifre doğruluğu tespit edilecektir. Bu sayede “1234”olan şifre bilgisi ele geçse dahi istenen şekilde yazılmadıkça uygulama kullanıcı girişine izin vermeyecektir.

## III. UYGULAMA

Çalışmada, hedeflenen amaç doğrultusunda, şifre girişi yapan kullanıcının tuşlarını ve tuşlara basma hızını takip edip veri tabanına kaydeden bir yazılım C# ortamında gerçekleştirilmiştir. Bu uygulama, önerilen yöntemin istenen düzeyde başarım gösterip göstermediğini belirlemek amacı ile hazırlanmış olup, oluşturulan bir şifrenin bilgisinin herhangi bir başka kullanıcı tarafından sisteme girmesi istenmiştir. Farklı kullanıcı tarafından aynı şifre girilmesine rağmen sistem şifreyi yazan kullanıcının kayıt yapan kullanıcı olmadığını tespit etmiştir. Hazırlanan program istenen sonuca başarılı bir şekilde ulaşmıştır. Yani bilgisayar sistemi program sayesinde girilen şifrenin aynı kodlama ve hızda olmadığını tespit etmiştir. Geliştirilen yazılımın çalışma şekli görsel olarak aşağıda anlatılmaktadır. Şekil 1’ de görüldüğü üzere programın ana formunda kullanıcı kayıt ve kayıt edilen kullanıcının programa girişini sağlayan iki düğme bulunmaktadır.



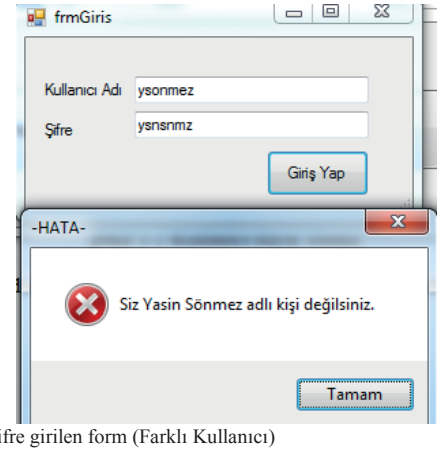

Şekil 1. Programın ana formu




Şekil 2. Kullanıcı kayıt formu

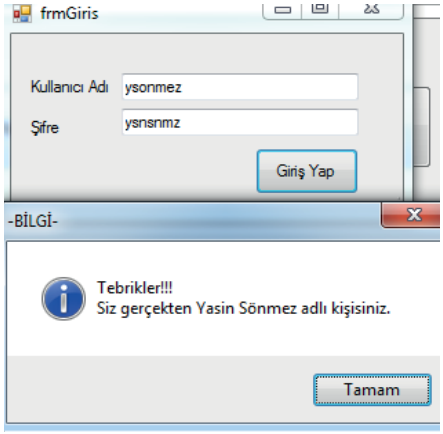
Şekil 2'de görüldüğü üzere kullanıcı kayıt formunda klavyeyi kullanarak kendi yazım tarzı ile şifresini yazmaktadır. Burada şifre "ysnsnmz" olarak belirlenmiş ve "ysn-snmz" şeklinde kodlanmış ve bu kod ile kullanıcının geliştirdiği hız tespit edilerek veri tabanına kayıt edilmiştir. Şifreler ilgili alanlarda normalde yıldızlı veya koyu siyah daireler şeklinde olurken programımızda şifreler açık şekilde belirtilmiştir. Bunun nedeni bir sonraki adımda aynı şifrenin girildiğini belirtmektir.

Bir önceki adımda girilen şifre veritabanına açık şekilde kayıt edilmiştir. Normal durumlarda kullandığımız programlar şifreleri veritabanlarına kayıt ederken belirli algoritmalara göre karıştırarak kaydetmektedir. Ancak veritabanları çalınsa dahi normal sistemlerde uygulanan algoritmaların tersi uygulandığında şifreler ele geçirilmektedir. Hazırlanan yazılımda şifrenin açık şekilde kayıt edilmesinin sebebi, veritabanları çalınır ve şifreler açık şekilde ele geçse dahi önerilen yöntem sayesinde şifrenin güvenli olduğunu ispatlamaya yöneliktir. Şekil 3'te, hazırlanan yazılımın, önerilen yöntemin hedefi doğrultusunda doğru bir şekilde çalıştığı görülmektedir. Şekil 2'de görülen şifrenin aynısı girilmesine rağmen önerilen yöntem sayesinde, yazılım şifreyi yazan kişinin doğru kişi olup olmadığını anlamakta ve uyarı iletisini göstermektedir. Bu şekilde farklı kişilerin doğu şifreyi bilmelerine rağmen sisteme girişleri engellenmektedir. Şifre yanlış kişi tarafından doğru girilmiş ve doğru kişi olup olmadığı kontrolü başarılı şekilde gerçekleştirilmiştir.




Şekil 3. Şifre girilen form (Farklı Kullanıcı)

Şekil 4'te de görüldüğü gibi şifre aynı kodlama ve hız ile girildiğinde, sistem şifreyi kabul etmiş yani sistem şifreyi kullanan kişi tarafından girilip girilmediğini kontrol etmiştir.




Şekil 4. Şifre girilen form (Şifreyi kullanan kişi tarafından girilmesi)

Önerilen yöntemin kullanılabilirliğinin test edilmesi amacıyla farklı ölçütler ile başarım oranı hesaplanmıştır. Bu ölçütler normal şifre kullanımları baz alınarak belirlenmiştir.

### A. *Metin tabanlı özgün kullanıcı şifresi.*

Programa daha önce bu programı kullanmış bir kullanıcının karakterlerden oluşan şifresi; on farklı kişiye yazılı olarak verilmiş ve şifreyi girmeleri istenmiştir. Kişilere verilen şifre on farklı kişi tarafından dört denemeden oluşacak şekilde girilmiştir. On farklı kişinin dört farklı denemesinden oluşan kırk farklı giriş isteğinin tümünde de doğru şifre girilmesine rağmen program şifreyi yazan kişinin doğru kişi olmadığını tespit etmiştir.

### B. *Sayı tabanlı özgün kullanıcı şifresi.*

Programa daha önce bu programı kullanmış bir kullanıcının rakamlardan oluşan şifresi; on farklı kişiye yazılı olarak verilmiş ve şifreyi girmeleri istenmiştir. Verilen şifre, on farklı kişi tarafından dört denemeden oluşacak şekilde girilmiştir. On farklı kişinin dört farklı denemesinden oluşan kırk farklı giriş isteğinin tümünde de doğru şifre girilmesine rağmen program şifreyi yazan kişinin doğru kişi olmadığını tespit etmiştir.

### C. *Metin-Sayı tabanlı denek kullanıcı şifresi.*

Programı ilk kez denek olarak kullanan kişilerden daha önce çeşitli platformlarda (masaüstü programlar, e-mail, web sayfaları vs.) kullandıkları şifrelerinin test için hazırlanan yazılıma kayıt edilmesi istenmiştir. Kaydettikleri kendi şifrelerini programa giren beş denek için yapılan testlerde elde edilen sonuçlar Tablo 1'de verilmektedir.

TABLO 1
METIN-SAYI TABANLI DENEK KULLANICI ŞIFRESI DENEME SONUÇLARI

| Kişi | 1. Deneme | 2. Deneme | 3. Deneme | 4. Deneme | Şifre Türü |
|---|---|---|---|---|---|
| 1 | Başarılı | Başarılı | Başarılı | Başarılı | Sayı |
| 2 | Başarısız | Başarılı | Başarılı | Başarısız | Metin |
| 3 | Başarısız | Başarısız | Başarılı | Başarılı | Metin-Sayı |
| 4 | Başarılı | Başarılı | Başarılı | Başarılı | Metin |
| 5 | Başarılı | Başarılı | Başarılı | Başarılı | Sayı |

Tablo 1'de görüldüğü üzere, sadece metin ve sadece sayı tabanlı oluşturulan şifrelerde güvenliğin yüksek düzeyde olduğu metin-sayı kombinasyonuna dayalı şifre kullanımlarında da yöntemin başarılı olduğu ancak başarı oranının biraz daha düştüğü gözlenmektedir.

## IV. SONUÇ

Bilgisayar kullanıcıları farkında olsun, olmasın klavye kullanarak yazı yazarken belirli tarzda yazmaktadırlar. Özellikle de çok sık kullanılan bazı bilgilerin klavye ile giriş tarzı kendini büyük ölçüde belirginleştirmektedir. Önerilen yöntem ile bilgisayarın kullanıcıyı tanıma boyutu; kişi - klavye kullanım tarzı kombinasyonunun güvenlik amacıyla kullanılması başarı ile gerçekleştirilmiştir. Böylece şifre yazarken klavye kullanım tarzının güvenlik amacıyla kullanılması fikrinin esasına dayanarak bir yazılım geliştirilmiş ve yapılan denemelerde başarılı sonuçlar üretmiştir.

Deneklerin geliştirilen sistem üzerindeki görüşleri alınırken oluşan fikirlerin ana teması: sistemin eğer sürekli kullandıkları klavye üzerinde denenmesi halinde tüm sonuçların başarılı olabileceği hakkında hemfikir oldukları gözlenmiştir. Bu fikrin ortaya çıkmasındaki temel sebebin kullanıcıların uzun süre kullandıkları klavye üzerinde klavye kullanım tarzı alışkanlıklarının daha da geliştiği fikri öne sürülebilir. Bu fikir çerçevesinde bu çalışmaya konu olan yazılımın şifre kullandığımız platformlarda (masaüstü programlar, e-mail, web sayfaları vs.) kullanılmasının güvenliğini arttıracağı konusunda başarılı olacağı düşünülmektedir. Önerilen yöntemin, güvenliği arttırmaya yönelik özelliğinin yanında caydırma, veritabanı çalınması gibi açıklara da çözüm sunacağı düşünülmektedir.

Önerilen yöntem doğrultusunda geliştirilen yazılım programının günlük kullandığımız programlarda (web sayfası üyelikleri, e-mail programları, Windows sürüm girişleri ve kredi kartı şifre girişlerinde vs. gibi) kullanılması ise ancak bu ara yüzleri yazılım programı olarak yapan kişiler tarafından önerilen sistemimizin kullanılması ile mümkün olacaktır.

Yapılan çalışma sonucunda geliştirilen şifreleme sistemi kullanıcının klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları saldırı yapan kişi/kişilere gönderen, keylogger olarak adlandırılan kötü amaçlı yazılımlara karşı; gelişen teknoloji ile yeni bir şifreleme tekniği olarak kullanılacağı tahmin edilmektedir.

## KAYNAKLAR

[1] G., Canbek, Ş. Sağıroğlu, "Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme", Gazi Üniversitesi Politeknik Dergisi, 9.3 (2006).

[2] Ü. A., Aydın, C., Acartürk. "Kullanılabilir Güvenlik ve Grafik Şifreler", Türkiyede İnternet Konferansı. 2012

[3] N. Özkaya, N., Sağıroğlu, Ş., "Açık Anahtar Altyapısı ve Biyometrik Sistemler", I. Ulusal Elektronik İmza Sempozyumu, 7–8 Aralık 2006, s.283-290, Ankara, Türkiye.

[4] R., Şamlı, M.E., Yüksel, "Biyometrik güvenlik sistemleri", Akademik Bilişim'09 (2009): 11-13.

[5] Korkmaz, İlker, and Mehmet Emin Dalkılıç. "Öncül Parola Denetimi Yöntemiyle Parola Seçim Sistemi: Türkçe Parolalar için Bir Araştırma."Akademik Bilişim'10: 206.

[6] G., Canbek. "Klavye dinleme ve önleme sistemleri Analiz, tasarım ve geliştirme", Yüksek Lisans Tezi. YÖK Tez No:184764, 2005

[7] Canbek, Gürol, and Şeref Sağıroğlu. "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", Gazi Müh. Mim. Fak. Dergisi 22.1 (2007): 121-136.

[8] Hilmi, G., Karabatak, M., "Online Bilişim Suçları ve Bu Suçlara Karşı Alınacak Önlemler", 1. Uluslar arası Adli Bilişim ve Güvenlik Sempozyumu, 20-21 Mayıs 2013, s. 120-125, Elazığ, Türkiye

[9] Öztürk, E., Duman, E., "Biyometrik Yöntemler ile Kimlik", 1. Uluslar arası Adli Bilişim ve Güvenlik Sempozyumu, 20-21 Mayıs 2013, s. 84-88, Elazığ, Türkiye

**Yasin Sönmez -** 1986 yılında Diyarbakır'da doğdu. 2010 yılında F.Ü. Bilgisayar Öğretmenliği Bölümünde lisans, 2012 yılında Elektronik ve Bilgisayar Eğitimi ABD'da yüksek lisans programını tamamladı. Halen F.Ü. Yazılım Mühendisliği ABD'da doktora öğrenimine devam etmekte olup Batman Üniversitesinde Öğretim Görevlisi olarak çalışmaktadır. (yasin.sonmez@batman.edu.tr)

**Murat Karabatak -** 1976 yılında Elazığ'da doğdu. 1999 yılında F.Ü. Bilgisayar Öğretmenliği Bölümünde lisans, 2002 yılında Elektronik ve Bilgisayar Eğitimi ABD'da yüksek lisans ve 2008 yılında Elektrik-Elektronik Mühendisliği ABD'da doktorasını tamamladı. Halen F.Ü. Yazılım Mühendisliği Bölümü'nde öğretim üyesi olarak görev yapmaktadır. (muratkar@hotmail.com)

**Engin Avcı -** 1978 yılında Elazığ'da doğdu. 2000 yılında F.Ü. Elektronik Öğretmenliği Bölümünde lisans, 2002 yılında Elektronik ve Bilgisayar Eğitimi ABD'da yüksek lisans ve 2005 yılında Elektrik-Elektronik Mühendisliği ABD'da doktorasını tamamladı. Halen F.Ü. Yazılım Mühendisliği Bölümü'nde öğretim üyesi olarak görev yapmaktadır. (enginavci23@hotmail.com)