

BIYOMETRİK GÜVENLİK SİSTEMLERİ VE YÜZ TANIMAYA DAYALI ÇEVİRİMİÇİ SINAV SİSTEMİ

Zihni Kaya
İstanbul Aydın Üniversitesi
UZEM, İstanbul
zihnikaya@aydin.edu.tr

Prof. Dr. Ali Güneş
İstanbul Aydın Üniversitesi
UZEM, İstanbul
aligunes@aydin.edu.tr

Özet

Bu çalışmada, çevrimiçi sınavlarda bir başkasının yerine sınava girişin önlenmesi amacıyla yüz tanımayla kimlik tespiti yapan bir uygulama geliştirilmiştir. Öncelikle ad, soyad ve yüz görüntüsü gibi verilerden oluşan kullanıcı bilgisi veri tabanına kaydedilmektedir. Sınav zamanında, kullanıcıdan web kamera yoluyla alınan yüz görüntüsü, veri tabanına daha önceden kaydedilen yüz görüntüsü ile karşılaştırılmaktadır. Karşılaştırma sonucuna göre kişi sınava alınmakta ya da alınmamaktadır. Günümüzde, hemen hemen her bilgisayarda bir web kamera olması, yüz tanımanın en güvenli biyometrik sistemlerinden biri olması ve kullanımı kolay olması nedeniyle bu çalışmada yüz tanıma sistemi kullanılmıştır. Bu çalışmada, otomatik insan yüzü tanımak için Özyüz yöntemi kullanılmış olup oldukça yüksek başarımler elde edilmiştir.

Anahtar Sözcükler: Biyometrik güvenlik sistemleri, yüz tanıma sistemi, çevrimiçi sınav sistemi.

BIOMETRIC SECURITY SYSTEMS AND FACE RECOGNITION BASED ONLINE EXAM SYSTEM

Abstract

In this study, an identification application based on face recognition is developed to prevent students from substituting others in online exams. Principally user information consisting data's such as name, surname and face image is saved on database. During the exam the face image of the user is taken by webcam and compared by the saved image data. Students' entry to exam will be accepted or denied according to the comparison result. Face recognition system is used in this study because almost every PC have web cam, face recognition is one of the most reliable biometric systems and also it is easy to use. In this study, eigenfaces method is used for automatic face recognition and considerably high success is achieved.

Keywords: Biometric security systems, face recognition system, online exam system.

GİRİŞ

Günümüzde kullanılan çevrimiçi sınav sistemlerinde kimlik tespiti genellikle kişiye daha önceden verilen bir anahtar (kullanıcı adı ve şifre gibi) ile yapılmaktadır. Bu anahtarı bilen herhangi bir kişi, o anahtarın gerçek sahibiymiş gibi sınava girebilmektedir. Bu yöntemde en büyük sorun bir başkasının yerine sınava girmeğidir.

Genellikle, uygulamalardaki gereksinimler, kullanıcı tanımlama ve bu tanımlamaya göre kullanıcıya sistemde hak verme şeklinde olmaktadır. Günümüzde, yaygın olarak kullanıcı tanımlama, numara ve manyetik kart gibi kişiye verilen bir karakter dizisi anahtar ile yapılmaktadır. Bu anahtar değerlerinin unutulabilir, kaybedilebilir veya tahmin edilebilir bir yapıda olması bu sistemlerin en büyük açığıdır.

Biyometrik sistemler bu eksiklikleri büyük ölçüde ortadan kaldıran sistemlerdir. Kişinin ölçülebilen fizyolojik veya davranışsal özelliklerine biyometri denilmektedir. Biyometrik sistemlerin en büyük üstünlüğü, bu özelliklerin unutulamayan, kaybedilemeyen ve tahmin edilemeyen yapılar olmasından kaynaklanır.

Bu çalışmada biyometrik güvenlik sistemlerinden yüz tanıma sistemi araştırılmış ve birçok kullanım alanı tespit edilmiştir. Bu sistemin, çevrimiçi sınav sistemlerinde de kimlik tespiti için kullanılabileceği örnek uygulama ile kanıtlanmıştır.

BIYOMETRİK GÜVENLİK SİSTEMLERİ

Biyometri (Biometric) Yunanca bio (yaşam) ve metric (ölçüm) sözcüklerinin birleşiminden meydana gelmiştir. Bireyin ölçülebilen fizyolojik veya davranışsal özelliklerine biyometri denir. Biyometrik sistemler, fiziksel özellikleri kullanılarak kişilerin elektronik ortamda tanınmasıdır. Biyometrik sistemler, bireylerden alınan örnekler ve uygulanacak algoritmalar ile birlikte bir depolama aygıtına saklanması sonrasında, verilerin eşleştirme prensibi ile çalışmaktadır (Varol & Cebe, 2011).

Başlıca biyometrik özellikler; yüz yapısı, parmak izi, avuç içi bilgisi, retina, iris, ses, yürüyüş, el yazısı, konuşma şekli ve DNA'dır.

Biyometrik sistemlerin en büyük üstünlüğü, bu özelliklerin unutulamayan, kaybedilemeyen ve tahmin edilemeyen yapılar olmasından kaynaklanmaktadır.

Herkeste farklı olan biyometrik özellikler, biyometriyi güvenlik sistemlerinde en çok tercih edilen bir alan haline getirmiştir. Biyometrik problemlerinden bilgisayarlı kimlik tespiti yapay zeka araştırmalarının önemli alanlarından biridir.

Biyometrik özellikleri kullanan sistemlere biyometrik sistemler denir. Bankacılık, güvenlik, kriminoloji gibi birçok alanda biyometrik sistemler kullanılmaktadır.

Biyometrik tanımlama yöntemlerinde kullanılan güvenlik sistemleri ile anlatılmak istenen şey aslında bilgi güvenliğidir. Bir bilginin güvenliği demek, bilginin gönderilmesi gereken kişiye değiştirilmeden, bozulmadan ve başka birisinin eline geçmeden ulaşması demektir. Bir bilgi gönderilmesi gereken kişi için gizli bir bilgi değilken 3. şahıslar için gizli bir bilgidir.

Biyometrik sistemler fizyolojik ve davranışsal biyometrik sistemler olmak üzere iki kısma ayrılır.

Davranışsal biyometrik sistemler imza, yazı dinamiği, yürüyüş şekli ve konuşma esnasındaki dudak hareketleri gibi belli zamanda belli amaçlar için gerçekleştirilmiş ve herkesin birbirinden farklı olarak gerçekleştirdiği davranışlar üzerine kurulmuştur (Şamlı & M. Erkal, 2009).

Fizyolojik biyometrik sistemler Fizyolojik biyometrik sistemler yüz, parmak izi, el geometrisi, DNA, ses, iris ve retina olmak üzere, bir kişinin diğer kişiden ayrılmasını sağlayan değişmez özellikler üzerine kurulmuştur.

Tablo 1’de biyometrik güvenlik sistemlerinin kullanılabilirlik özellikleri yüksek, orta ve düşük olarak sınıflandırılarak karşılaştırılmıştır (Yalçın & Gürsel, 2015). Bu çizelgede; Y=Yüksek, O=Orta, D=Düşük olarak ifade edilmektedir.

Tablo 1: Biyometrik Güvenlik Sistemlerinin Kullanılabilirlik Özelliklerine Göre Sınıflandırılması

	Evrensellik	Eşsizlik	Süreklilik	Elde Edilebilirlik	Performans	Kabul Edilebilirlik	Yaygınlık
İmza	D	D	D	Y	D	Y	Y
Parmak izi	O	Y	Y	O	Y	O	O
DNA	Y	Y	Y	D	Y	D	D
İris	Y	Y	Y	O	Y	D	D
Ses	O	D	D	O	D	Y	Y
Yüz	Y	D	O	Y	D	Y	Y

Tablo 1’de görüldüğü gibi, imza biyometriğinin evrensel özelliği düşüktür. Organ kaybı gibi sebeplerden dolayı imza atma yeteneğinin olmaması veya okuma yazma bilmeyenlerin kendilerine ait bir imza biçiminin bulunmaması nedeniyle bu özellik düşüktür. DNA, iris ve yüz biyometriklerinin sahip oldukları özellikler yönünden evrensellikleri yüksek olarak sınıflandırılmıştır.

Her insanda farklı olması yani eşsizlik özelliği yönünden baktığımızda DNA, parmak izi ve iris biyometrikleri aynı yumurta ikizlerinde bile farklı olduğundan yüksek olarak sınıflandırılmıştır.

Yaşam boyunca değişmeyen yani süreklilik özelliği bakımından değerlendirildiğinde DNA, parmak izi ve iris biyometrikleri yüksek olarak sınıflandırılmıştır. İmza ve ses biyometrikleri ise neşe, heyecan, korku ve soğuk hava gibi değişimlere bağlı olarak değiştikleri için düşük olarak sınıflandırılmışlardır.

Gözün narin yapısı ve kullanılan cihazın verdiği rahatsızlık gibi nedenlerden dolayı iris biyometriğinin elde edilebilirliği düşüktür. Yüz ve imza biyometriklerinin elde edilebilirliği ise yükseltir.

Doğruluk ve hız yönünden DNA, parmak izi ve iris biyometriklerinin performansı yüksektir.

Biyometrik verilerin ölçüm ve toplanması yönünden yani kabul edilebilirlik bakımından yüz, ses ve imza biyometrikleri yüksek sınıflandırılmıştır.

Son olarak yüz, imza ve ses biyometrikleri yaygınlık bakımından yüksek olarak sınıflandırılmıştır.

YÜZ TANIMA YÖNTEMLERİ

Yüz tanıma; güvenlik sistemlerinde, suçluların izlenmesinde ve çok gizli yerlere giriş-çıkışların denetlenmesi gibi bir çok alanda kullanılmaktadır. Bir bilgisayarın yüz tanımayı gerçekleştirebilmesi yapay zeka araştırmacılarını ilgilendiren önemli konulardan biridir.

Bilgisayarlı yüz tanımanın uzun bir geçmişi vardır. Çoğu yüz tanıma yöntemi yüzleri; göz köşeleri, ağız kenarları ve burun ucu gibi özellik noktaları arasındaki normalize edilmiş uzunluklara ve oranlara göre modeller ve sınıflandırır (Nabiyev, 2012).

Yüz tanıma problemi üç grupta incelenebilir:

- Yüz Bulma

- Yüz Normalleştirme
- Yüz Onaylama

Yüz tanıma sisteminin başarımında sistemin hızı ve yanlış tanıma oranı dikkate alınmaktadır. Yüz tanıma sisteminde karşılaşılan sorunlardan aydınlatma problemi ve pozların çok çeşitli olması öne çıkmaktadır. Işıklandırma nedeniyle yüz tanınamayabilir. Bu sorunun çözümü için ışıklandırma konileri kullanılmaktadır (Nabiyev, 2012).

Yüz tanımda özellikler bilindiğinde; yapay sinir ağları, radyal alt fonksiyon ağları, çok katmanlı perspektif, doğruluk haritaları, esnek demet graf eşlemesi, en önemli parçaların farkını bulma ve birçok temsilci gibi yaklaşımlardan herhangi birisi kullanılabilir. Yüz tanımda en başarılı yöntemlerden birisi iki boyutlu resimlerden global özelliklerin elde edilmesidir.

Yüz tanıma algoritmaları içinde en yaygın kullanılan yaklaşım özyüz (eigenfaces) tabanlı yöntem olup bu çalışmada da uygulanmıştır. Yüz görüntülerinin ayırt edici karakteristik özellikleri kullanılarak mümkün olduğunca küçük boyutlu bir uzay oluşturulur ve görüntüler bu yüz uzayında karşılaştırılır. Bu uzayın özyüzler olarak adlandırılan temel vektörleri, yüzlerin bazı yerel ve global özelliklerini meydana çıkarırlar ve yüz görüntülerinin içeriğiyle ilgili bilgi verirler (Turk & Pentland, 1991).

Bilgisayarda yüz tanıma sistemiyle ilgili araştırmaların uzun bir geçmişi. Başlıca biyometrik teknolojilerden biri olan yüz tanıma, görüntü yakalama cihazlarındaki hızlı gelişmeler ve yüksek güvenliğe olan ihtiyaçlar sonucunda, giderek daha önemli bir hale gelmiştir.

Bir insanın yüzü kendine hastır. Dolayısıyla, kimliğinin tespitinde bu karakteristik özellikleri kullanılabilir. Yüz tanıma teknolojisinin çalışma mantığı yüz görüntülerinden karakteristik özelliklerin çıkarılmasına dayanır. Sonrasında ise, iki görüntü karşılaştırılır (Varlık & Çorumluoğlu, 2011).

Yüz tanıma süreci yüz görüntülerinden çeşitli özelliklerin çıkarılmasıyla başlar. Aynı kişinin yüz görüntülerinin özellikleri arasında bir benzerlik olurken, farklı kişilerin yüz görüntülerinin özellikleri arasında farklılık olur. Bütün bunlar dikkate alındığında yüz tanıma sistemleri “özellik tabanlı” ve “görünüm tabanlı” olmak üzere iki ayrı yolla incelenebilir.

Özellik tabanlı yüz tanıma sistemleri: Geometrik özellik tabanlı, şablon eşlemeli yöntem, yapısal eşleme, gizli Markov modeli, dalgacık dönüşüm ve elastik demet grafi eşleme gibi yüz tanıma yöntemleri vardır.

Görünüm tabanlı yüz tanıma sistemleri: Özyüz yaklaşımı (Turk & Pentland, 1991), Fisher yaklaşımı (Belhumeur, Hespanha, & Kriegman, 1997) ve yapay sinir ağı gibi yüz tanıma yöntemleri vardır.

Öncelikle “geometrik özellik tabanlı” ve “şablon eşlemeli” yüz tanıma yöntemleri kısaca ele alındıktan sonra, bu çalışmada kullanılan önyüz yöntemi üzerinde durulacaktır.

Geometrik Tabanlı Yüz Tanıma

İlk yüz tanıma yöntemi olan geometrik tabanlı yüz tanıma sistemi Goldstein tarafından 1964 yılında kullanılmıştır. Yüzde belirleyici özelliğe sahip bölgelerin boyutlarının birbirleri ile arasındaki uzaklıkların ve geometrisinin hesaplanması ile yapılan tanımlama yöntemidir.

Kaya ve Kobayashi (1972) yüz üzerindeki belirli noktaların belirlenmesinde birtakım önemli etmenler belirlemiş ve bu noktalar arasındaki öklit uzaklığını hesaplamışlardır (Brunelli & Poggio, 1992).

- Kolay tahmini edilebilmeli
- Işığa az duyarlı olmalı
- Mimikten mümkün olduğunca bağımsız olmalı
- Ayırt edici özelliğe sahip bilgi mümkün olduğunca çok olmalı

Yüz üzerindeki tanımlayıcı özelliğe sahip noktalara örnek olarak göz, ağız, kaş, çene ve burun örnek olarak verilebilir.

Geometrik özellik tabanlı yüz tanıma yöntemleri, daha önceden tanımlanmış kaş kalınlığı ve dikey konumu, burun kalınlığı ve konumu gibi ayırıcı özellikleri kullanır. Bulunan değerler özellik vektörü olarak kaydedilir. Brunelli ve Poggio 1992 yılında, yüzün ayırıcı özellikleri olarak gördükleri 22 geometik noktayı belirlemişlerdir.

Bu geometrik noktalardan elde edilen 22 tane değer en yakın komşuluk algoritması kullanılarak karşılaştırılır ve en küçük değere sahip veri tabanı resmi ile eşleştirilir. (Brunelli & Poggio, 1992).

Şablon Eşlemeli Yöntem

Bu yöntemde, iki farklı desenin tümü veya belirli özelliklerdeki parça şablonları en yakın komşuluk algoritması ile karşılaştırılır (Brunelli & Poggio, 1993). Şablon eşlemeli yöntemde görüntüler gri renk düzleminde. Eşleme algoritması, eğitim ve test veri kümeleri arasındaki farklılıkları ve benzerlikleri hesaplar. Eşleme, görüntünün belirli kısımlarına veya bütün görüntüye uygulanmalıdır. Şablonlar, görüntüler arasındaki benzerliklerin en çok olduğu veya farklılıkların en çok olduğu bölümlerden seçilir (Brunelli & Poggio, 1995). Şablon desenleri, eğitim verilerinden alınan referans desenleri olarak kabul edilir. Bir test resmi, bu referans desenleri kullanılarak tanımlanmaya çalışılır. Sonuçta, eğitim ve test desenleri arasındaki benzerlikler ve farklılıklar hesaplanır (Brunelli & Poggio, 1993).

Özyüz Yaklaşımı

Gerçek hayatta, bir görüntü iki boyutlu bir $f(x,y)$ fonksiyonu olarak tanımlanır. Burada x ve y düzlemsel koordinatlarıdır. f fonksiyonunun herhangi bir (x,y) koordinatındaki genliği görüntünün o noktadaki yeşinlik (örneğin parlaklık gibi) veya gri seviyesi olarak adlandırılır. x , y , f 'in yeşinlik değerleri hep birlikte sonlu ve ayrık büyüklükte olduğunda bu görüntüye sayısal görüntü denir (Gonzalez & Woods, 2014). Sayısal görüntü sonlu sayıda bileşenden oluşur. Her bir bileşen belli bir görüntünün değeridir. Bu bileşenlere resim elemanı, görüntü elemanı veya piksel denir.

Yüz tanıma algoritmaları içinde en yaygın kullanılan yaklaşım özyüz (eigenfaces) tabanlı yöntemlerdir. Yüz görüntülerinin ayırt edici karakteristik özellikleri kullanılarak mümkün olduğunca küçük boyutlu bir uzay oluşturulur ve görüntüler bu yüz uzayında karşılaştırılır. Bu uzayın özyüzler olarak adlandırılan temel vektörleri, yüzlerin bazı yerel ve global özelliklerini meydana çıkarırlar ve yüz görüntülerinin içeriğiyle ilgili bilgi verirler (Turk & Pentland, 1991).

Özyüz algoritması (Temel bileşenler analizi) boyut azaltmak ve görüntüler arasındaki temel farklılıkları bulmak için kullanılan bir yöntemdir (Turk & Pentland, 1991). Temel bileşen analizi sınıf bilgisini kullanmadığı için gözetimsiz bir öğrenme yöntemidir. Ölçüt, verideki varyanstır. Veri noktaları arasındaki farkın en iyi ortaya çıktığı, yani varyansın en yüksek olduğu vektör temel bileşeni oluşturur (Alpaydın, 2012, s. 90-92). Özyüz algoritmasında her biri $N \times N$ boyutunda olan görüntüler N^2 uzunluğunda vektörlere dönüştürülür. Bu çalışmada da kullanılan Özyüz algoritmasının işlevsel blok şeması Şekil 1'de verilmiştir (Erdoğan, 2010).

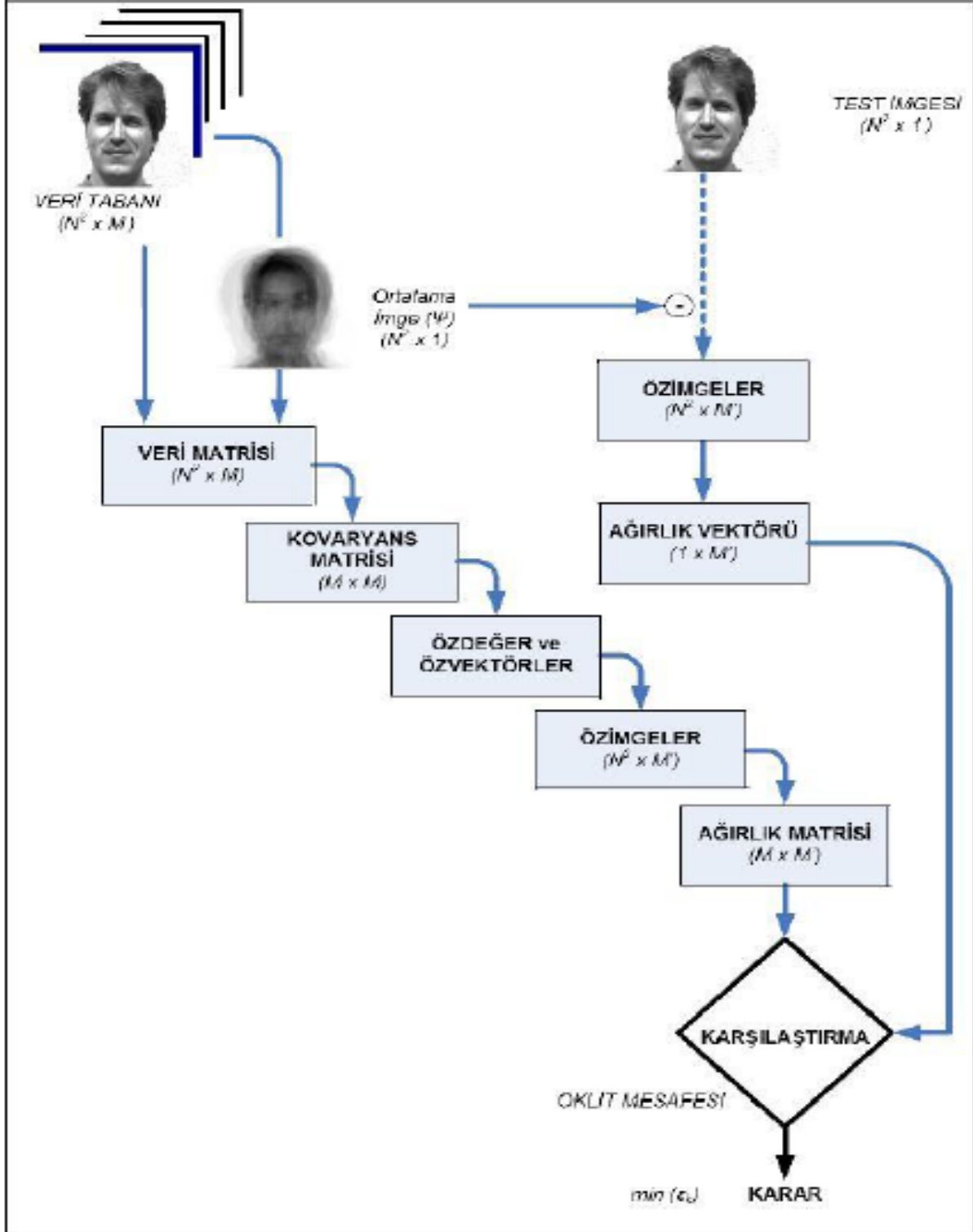
YÜZ TANIMA TEKNOLOJİSİYLE ÇEVİRİMİÇİ SINAV SİSTEMİ

Çevrimiçi eğitim sistemlerinde ölçme ve değerlendirme, genellikle, çevrimiçi sınav sistemleri ile yapılmaktadır. Sınav soruları çoktan tek seçmeli, çoktan çok çekmeli, doğru-yanlış, kısa cevap, boşluk doldurma, numaralı vb. türünde olmaktadır.

Sınav soruları ve cevapları ilgili öğretmen veya sistem görevlisi tarafından soru bankasına girilir. Bu sorular ve cevapları web sunucudaki bir veri tabanında tutulur.

Daha önceden belirlenen gün ve saatte, sınav sistemine başarıyla giriş yapan öğrencilerin ekranına, soru bankasından rastgele seçilen sorular gelir. Soru bankasından her öğrenciye eşit sayıda, aynı zorluk seviyesinde, rastgele sorular seçilir. Öğrencinin ekranına sorular ve cevap seçenekleri rasgele sıralamada çıkartılır. Böylece, birbirine bakarak kopya çekmenin önüne geçilmeye çalışılır. Bu bağlamda soru bankasında ne kadar çok soru varsa, birbirine bakarak kopya çekme o kadar zor olur.

Öğrencilerin sınav süresi içinde cevapladığı sorular, sınav uygulaması tarafından sunucudaki veri tabanına kaydedilir.



Şekil 1: Özyüz Algoritması İle Sınıflandırma İşlevsel Blok Şeması

Sınav sistemine giriş için öğrenciler kendilerine daha önceden verilen bir kullanıcı adı ve şifre kullanırlar. Bir kişi diğer kişinin kullanıcı adı ve şifresini biliyorsa onun yerine sınava girebilir. Bu çalışmada, bu sorunun çözümü için otomatik kimlik tanımlama yöntemlerinden yüz tanıma sistemi araştırılmış ve yüz tanıma teknolojisi kullanılarak güvenli çevrimiçi sınav uygulaması geliştirilmiştir.

Merkezi bir veri tabanı ve yüz tanıma sistemi ile otomatik olarak sınav girişinin kontrol edilmesi ve işletilmesi gerçekleştirilmiştir. Her bilgisayarda bulunan ve donanım olarak kullanılan web kamera ile kişilerin görüntüleri alınmakta, sonrasında ise bu görüntü ile veri tabanındaki yüz görüntüleri karşılaştırılarak sınav giriş kontrolü yapılmaktadır. Böylece, klasik olarak yapılan kimlik tespit yöntemlerine alternatif olarak çevrimiçi çalışan, kontrolü yapılabilen, otomatik olarak kimlik tespiti yapabilen ve yüz görüntülerinden kimlik oluşturabilen öğrenci tanıma uygulaması geliştirilmiştir.

Bu projede, kimlik tespiti internet üzerinden veya yerel ağ üzerinden yapıldığından zamandan tasarruf sağlayacaktır. Ayrıca, çok fazla öğrencinin bulunduğu sınavlarda, gözetmenler tarafından tanınmayan öğrenciler, sistem tarafından otomatik olarak tanınacağından sınav güvenliği de artacaktır.

Biyometrik tanımlama yoluyla yüz görüntülerinden oluşturulan kimlik bilgisi sisteme eklenecek ve bir merkezi yönetim ile öğrenci girişleri otomatik olarak yapılacaktır. Veri tabanında kimlik bilgisi olmayan kişilere sınav ekranı açılmayacak, böylece, bir başkasının yerine sınava girme şeklinden yapılan sınav hileleri ortadan kalkacaktır.

Yüz Tanıma İle Sınav Giriş Uygulamasında Kullanılan Yazılım Yapısı

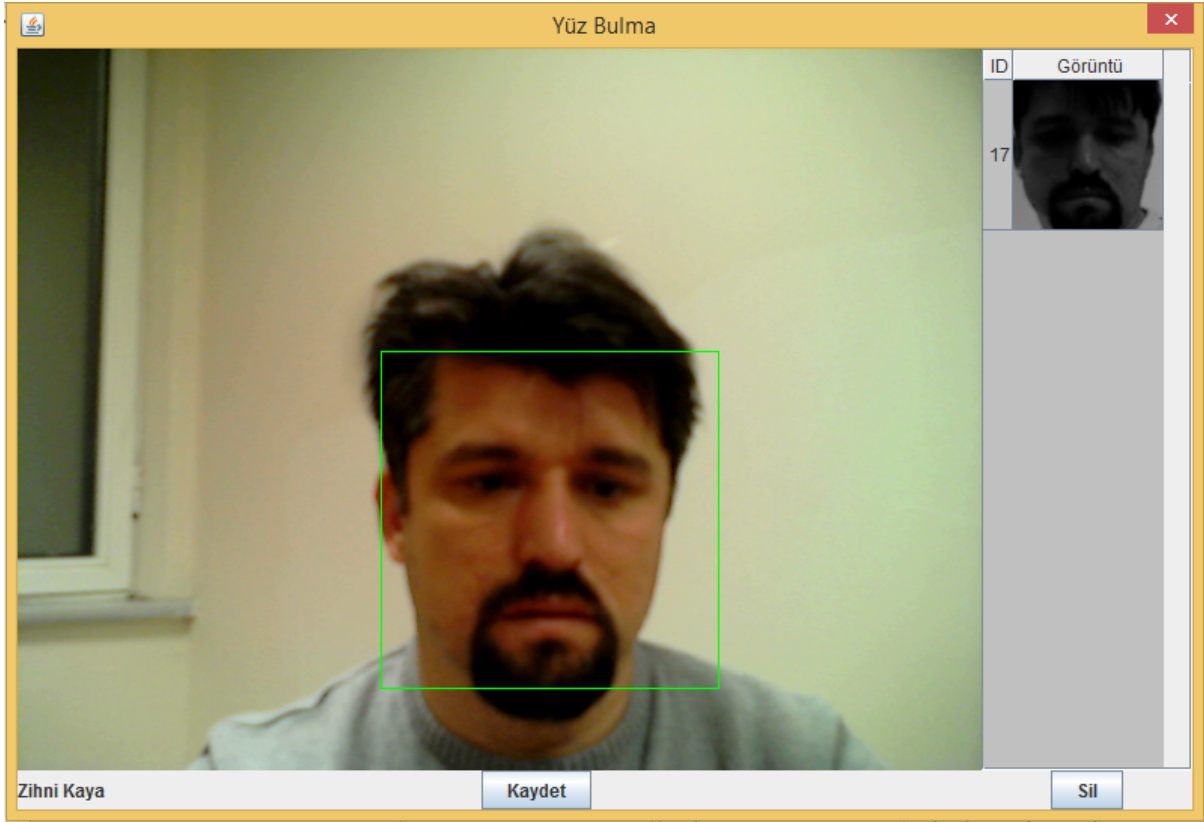
Bu projede, Java programlama dili kullanılarak, sınav sisteminde tanımlanan kullanıcı bilgileri ile web kameradan gelen yüz görüntüsü bilgilerini yöneten bir sistem geliştirilmiştir. Görüntü işleme kütüphaneleri olarak OpenCV ve JavaCV kullanılmıştır.

OpenCV Intel tarafından geliştirilerek BSD lisansı ile lisanslanmış, “Bilgisayarla Görü/ Görme” kütüphanesidir. Özellikle gerçek zamanlı uygulamalar hedef alınarak geliştirilmiş olması, ticari kullanımı dahil ücretsiz olması ve Windows, Linux, MacOS X gibi farklı platformlarda kullanılabilmesi bu kütüphaneyi diğer görüntü işleme araçlarından bir adım öne çıkarmaktadır (Erişti, 2010).

Sınav giriş ekranı Java programlama dili kullanılarak geliştirilmiştir. Bu ekranda yapılan kimlik tespitinden başarıyla geçen kullanıcılar PHP ile geliştirilen sınav uygulamasına yönlendirilirler. Veri tabanı olarak MySQL sunucu kullanılmıştır.

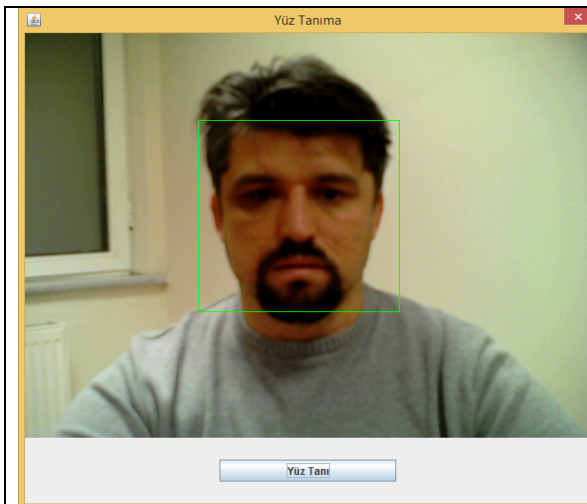
Uygulama, yönetici ve kullanıcı ekranlarından oluşur. Yönetici giriş arayüzü, yöneticisi yetkisine sahip olan kullanıcıların sisteme giriş yaptığı ekrandır. Yönetici ana ekranı arayüzü, kullanıcı ekleme, düzenleme, silme ve yüz görüntüsü ekleme gibi işlemlerin yapıldığı yönetici ana ekranıdır. Bu ekrana ilk giriş yapıldığında sistem veri tabanında kayıtlı olan tüm öğrenciler listelenir.

Yeni kullanıcı ekleme arayüzü ile sisteme yeni kullanıcı eklenir. Kullanıcı yüz bulma arayüzü, sistemde yer alan bir kullanıcı için yüz görüntüsü bulmak amacıyla kullanılır. Şekil 2’de örneği gösterilen bu arayüze giriş yapıldığında web kamera çalıştırılmakta yakalanan görüntüdeki yüz bulunarak yeşil kenarlı dikdörtgen içine alınmaktadır. “Kaydet” düğmesine tıkladığında, bulunan yüz görüntüsü 100x100 piksel boyutlarında görüntüye dönüştürülür. Sonrasında, RGB renk uzayındaki görüntü Gri seviye görüntüye çevrilir. Son olarak, JPEG görüntü formatında veri tabanına kaydedilir. Ekranın sağ tarafında, ilgili kullanıcının veri tabanında bulunan tüm yüz görüntüleri listelenmektedir. Buradaki yüz görüntüleri kullanılarak kişinin kimlik bilgileri oluşturulur. Yüz tanımda kullanılmak istenmeyen yüz görüntüleri “Sil” düğmesine tıklanarak veri tabanından silinir.

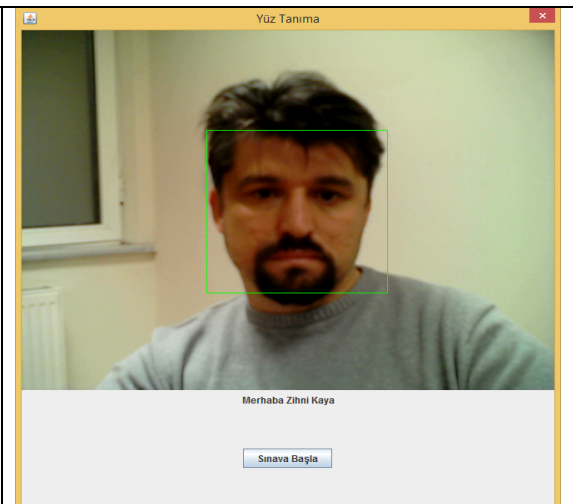


Şekil 2: Kullanıcı Yüz Görüntüsü Bulma Arayüzü

Kullanıcı Giriş Arayüzü: Sisteme daha önceden kayıt olmuş öğrencilerin sınava girmek için kullandıkları arayüzdür. Kullanıcı giriş arayüzü görüntüsü Şekil 3'te gösterilmiştir. Bu arayüz ile web kameradan gelen görüntüler alınmakta ve bu görüntülerdeki yüz bulunmaktadır. Kullanıcı "Yüz Tanı" düğmesine tıklayarak yüz tanıma işlemi başlatır. Yüz tanıma JavaCV kütüphanesi kullanılarak gerçekleştirilmiştir (JavaCV, OpenCV için bir Java arayüzüdür). Bulunan yüz görüntüsü veri tabanında kayıtlı olan yüz görüntüleriyle eşleştirilmektedir. Eşleştirme sonucuna göre, öğrencinin sınava girişine izin verilmekte ya da verilmemektedir. Eşleştirme sonucunu gösteren ekran görüntüsü Şekil 4'te görülmektedir. Burada yer alan "Sınava Başla" düğmesine tıklayarak sınav uygulamasına geçiş yapılır.



Şekil 3 : Kullanıcı kimlik tespiti arayüzü



Şekil 4: Kullanıcı kimlik tespiti sonucu

Sınav Arayüzü: Kimlik tespitinden başarıyla geçen öğrencilerin sınav oldukları web tabanlı uygulamadır. Uygulamanın ekran görüntüsü Şekil 5'te görülmektedir.

BİLİŞİM TEKNOLOJİSİ-1 Kalan süre: 16 dk. 54 sn.

1.(14577) Aşağıdakilerden hangisi bilgisayarı oluşturan ana donanım birimlerinden **değildir**?

Modem
 Klavye
 Monitör
 Anakart

ZİHNİ KAYA
Y1313.010023

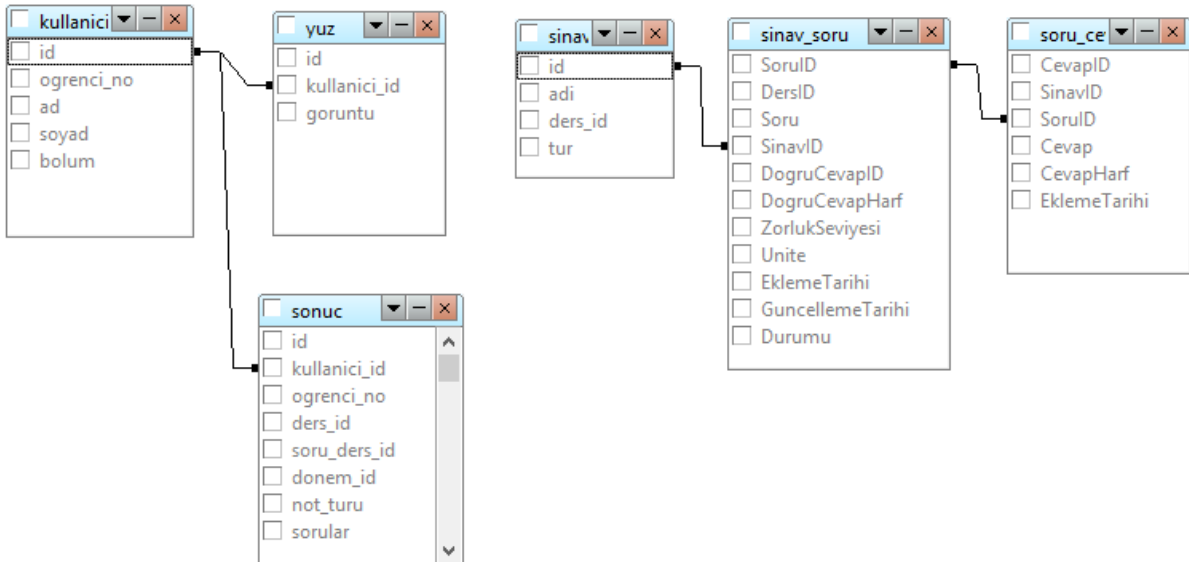
Önceki Soru 1 / 20 Sonraki Soru

Cevapları Gör ve Sınavı Bitir

Şekil 5: Sınav Arayüzü

Sınav Sisteminin Veri Tabanı Yapısı

Sınav sisteminde kullanılan veri tabanı yapısı Şekil 6'da görülmektedir. "yuz" tablosu, 100x100 piksel boyutlarındaki gri seviye yüz görüntülerinin ikili olarak saklandığı BLOB tipinden bir alandır.



Şekil 6: Sınav Sistemi Veritabanı Yapısı

SONUÇ VE ÖNERİLER

Bu çalışmanın amacı, bir kişinin başka bir kişinin yerine sınava girerek sahtekarlık yapmasını önlemektir.

Bu çalışmada, biyometrik güvenlik sistemlerinden yüz tanıma sistemi araştırılmış ve bir çok kullanım alanı tespit edilmiştir. Bu sistemin, çevrimiçi sınav sistemlerinde de kimlik tespiti için kullanılabileceği örnek uygulama ile kanıtlanmıştır.

Bilgisayar tabanlı sistemlerde yapılan sınavlarda, özellikle gözetmenler tarafından tanınmayan öğrencilerin sınavlara girişinde problemler yaşanabilmektedir. Bu sınav sistemlerinde genellikle, sınava giriş hakkı, kullanıcıya daha önceden verilen bir anahtar (kullanıcı adı ve şifre gibi) doğrulanarak verilmektedir. Bu anahtarı bilen herhangi bir kişi, o anahtarın gerçek sahibiymiş gibi sınava girebilmektedir. Buda, başkasının yerine sınava girme problemini ortaya çıkarmaktadır. Bu çalışma ile bu problemin önüne geçilmiştir.

Öncelikle, sınav sistemine giriş yapacak kişilerin ad, soyad, öğrenci numarası ve yüz görüntü bilgilerinden oluşan kimlik bilgileri veri tabanına kaydedilmektedir. Yüz görüntüleri 100x100 piksel boyutlarında ve gri ölçekte tutulur.

Sınav zamanında, web kamera yoluyla alınan yüz görüntüsü veri tabanındaki yüz görüntüleri ile karşılaştırılır. Bu karşılaştırma sonucuna göre öğrenciye sınava giriş hakkı verilmekte ya da verilmemektedir.

50 öğrenci sisteme tanımlanmış ve her bir öğrenci için bir tane yüz görüntüsü veri tabanına kaydedilmiştir. Sistem, bu 50 kişiden 40'ının kimlik tespitini doğru olarak yapmıştır.

Kalan 10 kişi için sisteme farklı pozlarda 5 yüz görüntüsü daha eklemiştir. Sonrasında, yüz tanıma sistemi bu kişilerden 8'inin kimlik tespitini doğru olarak yapmıştır. Geri kalan 2 kişi yanlış tanınmıştır.

Not: Bu çalışma 5- 6 Şubat 2016 Tarihlerinde Antalya'da düzenlenen 2nd International Congress on Education, Distance Education and Educational Technology- ICDET'de sözlü bildiri olarak sunulmuştur.

KAYNAKÇA

Alpaydın, E. (2012). *Yapay Öğrenme*. İstanbul: Boğaziçi Üniversitesi Yayınevi.

Belhumeur, P., Hespanha, J., & Kriegman, D. (1997). Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. *IEEE Transaction On Pattern Analysis and Machine Intelligence*, 19(7), 711 - 720.

Brunelli, R., & Poggio, T. (1992). Face recognition through geometrical features.

Brunelli, R., & Poggio, T. (1993). Face recognition: Features versus templates. *IEEE Transaction on Pattern Analysis and Machine Intelligence*, 15, 1042-1053.

Brunelli, R., & Poggio, T. (1995). Template Matching: Matched Spatial Filters and Beyond. *IRST Tech. Rep.*

Erdoğan, A. Y. (2010). Yüz Tanımda Özyüz ve Fisher Yüz Algotimalarının İncelenmesi. *Yüksek Lisans Tezi*, 28. Ankara: Ankara Üniversitesi, Fen Bilimleri Enstitüsü.

Erişti, E. (2010). Görüntü İşlemede Yeni Bir Soluk, OPENCV. *Akademik Bilişim'10*, (s. 223-228). Muğla.

Gonzalez, R., & Woods, R. (2014). *Sayısal Görüntü İşleme* (3.Baskıdan Çeviri b.). Ankara: Palme Yayıncılık.

Kaya, Y., & Kobayashi, K. (1972). A basic study on human face recognition. *Frontiers of pattern recognition*, 265-289.

Nabiyev, V. V. (2012). *Yapay Zeka*. Ankara: Seçkin Yayıncılık.

řamlı, R., & M.Erkal, Y. (2009). Biyometrik Güvenlik Sistemleri. řanlıurfa: XI Akademik Biliřim Konferansı.

Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, 3(1), 71-86.

Varlık, A., & Çorumluođlu, Ö. (2011). Dijital Fotogrametri Teknikleri İle Kiři Tanıma. *Harita Teknolojileri Elektronik Dergisi*, 3(2), 1-24.

Yalçın, N. (2008, Mart). Konuřma Tanıma Teorisi ve Teknikleri. *Kastamonu Eđitim Dergisi*, s. 249-266.

Yalçın, N., & Gürsel, F. (2015). Biyometrik Güvenlik Sistemlerinin İncelenmesi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 398-413.