İleri Teknoloji Bilimleri Dergisi
Journal of Advanced Technology Sciences
ISSN:2147-3455

BİYOMETRİK VERİ BİRLEŞTİRME YÖNTEMLERİ

UMAS 2017'de sunulmuş ve genişletilmiş bildiridir.

Aykut DURGUT[1] Serdar BİROĞUL[2]

[1] Balıkesir Üniversitesi, Altınoluk Meslek Yüksekokulu, Bilgisayar Programlama Bölümü, 10870, Balıkesir, TÜRKİYE
[2] Düzce Üniversitesi, Teknik Eğitim Fak., Bilgisayar Mühendisliği Bölümü, 81620, Düzce, TÜRKİYE

Özet-Biyometrik yetkilendirme yöntemlerinde tek biyometrik veri yetersiz kalmaktadır. Bu yüzden birden fazla biyometrik veri kullanılmaktadır. Birden fazla kullanılan biyometrik verinin korunmasında ise çeşitli birleştirme yöntemleri ile tek şablon oluşturulmaktadır. Bu çalışmada, literatürdeki biyometrik birleştirme yöntemleri incelenerek avantajları ve sınırlılıkları belirlenmiştir. Aynı zamanda biyometrik birleştirme yöntemleri için öneriler sunulmuştur.

Anahtar Kelimeler- Biyometrik Şablon, Biyometrik füzyon, Biyometrik birleştime, Biyometrik şifreleme, Biyometri.

BİOMETRİC FUSİON METHODS

Abstract-In biometric authentication methods, only one biometric data is insufficient. Therefore, more than one biometric data is used. In the preservation of more than one used biometric data, a single template is created by various combining methods. In this study, the advantages and limitations of the biometric combining methods in the literature were examined. At the same time, suggestions for biometric integration methods are presented.

Key Words- Biometric template, Biometric fusion, Biometric encryption, Biometric.

1. GİRİŞ (INTRODUCTION)

Biyometrik yetkilendirme, kişiye ait fiziksel ve biyolojik özellikleri kullanarak çeşitli sistemlere giriş yapılabilmesi için kullanılan yöntemdir. Biyometrik yetkilendirme sistemleri, şifre ve kartlı yetkilendirme sistemlerine göre daha güvenilirdir. Biyometrik sistemlerin temelinde kişiye has olan, herhangi biri tarafından değiştirilemeyen, kişinin kendisi olduğunu kanıtlamaya yarayan, kişiyi diğer kişilerden ayıran fiziksel ve davranışsal özelliklere dayanmaktadır. Biyometrik sistemlerin fiziksel ve davranışsal özelliklerden oluşmasının nedeni bu özelliklerinin kaybolmaması, başka kişiler tarafından kullanılamaması ve taklit edilememesidir. Biyometrik yetkilendirme ile kimlik tespiti yapılabilmesi için şifre ezberlemek zorunda kalmadan, taklit edilemeyen özellikler kullanılarak işlem yapılabilmektedir [1].

Kişiye özel olan biyometrik verilerden çeşitli yöntemlerde kullanılan biyometrinin öznitelik noktaları çıkarılmaktadır. Çıkarılan bu öznitelikler şablon olarak isimlendirilmekte ve sisteme girilen yeni biyometrik bilgiden elde edilen şablon ile karşılaştırılmaktadır. Karşılaştırmanın

sonucunda kayıtlı şablon ile yeni üretilen şablon eşleştirildiğinde yeterli seviyede eşleşme gerçekleşirse kullanıcıya giriş izni verilmektedir [1].

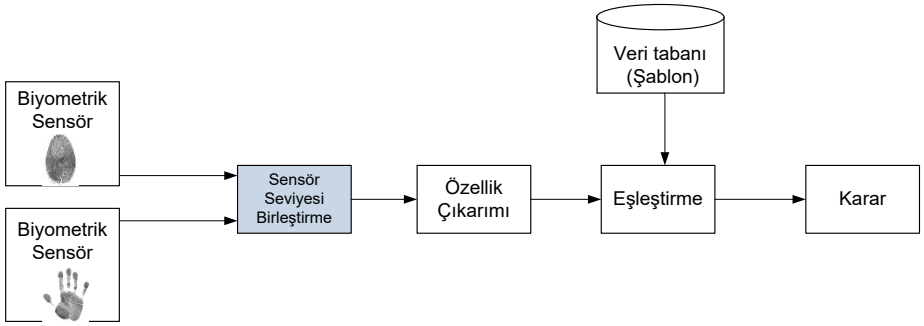
2. ÇOKLU BİYOMETRİK SİSTEMLER (MULTI-BIOMETRIC SYSTEMS)

Biyometrik yetkilendirme sistemlerinde tek biyometrinin kullanılması sorunlara yol açmaktadır. Bunlardan bazıları biyometriden elde edilen şablonda yeteri kadar öznitelik elde edilememsi ve karşılaştırmada aynı kişiyi tanıyamaması, diğer sorun ise tek biyometrinin taklit edilebilmesinin daha kolay olmasıdır [1]. Bunun gibi sorunlardan dolayı yetkilendirme sistemlerinde farklı biyometrik özelliklerden yararlanılmaktadır.

Kullanıcıdan alınan farklı biyometriler ayrı ayrı tutulmak yerine birleştirilerek tek şablon şeklinde tutulmaktadır. Farklı biyometrik bilgiler sistemin çeşitli aşamalarında birleştirilmiştir. Bunlar: sensör seviyesi, özellik seviyesi, eşleştirme seviyesi, karar seviyesidir.

2.1. Sensör Seviyesi Birleştirme (Sensor Level Fusion)

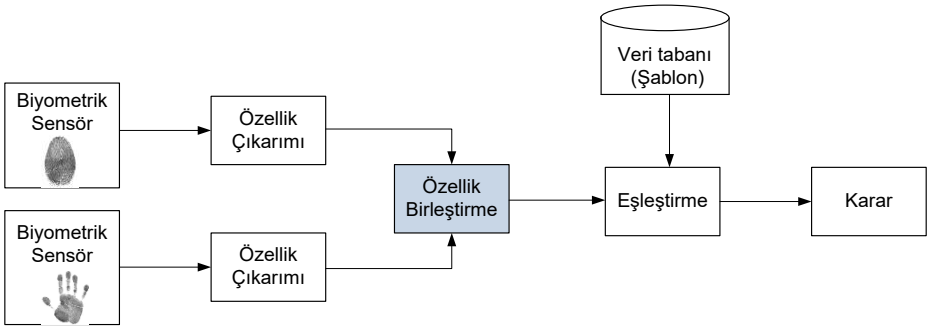
Sensörlerden alınan ham verinin birleştirilmesidir. Şekil 1'de görüldüğü gibi aynı biyometrik örneğin uygun farklı sensörlerden veya aynı sensörden elde edilen verilerin birleştirilmesidir.



Şekil 1. Sensör Seviyesi Birleştirme

2.2. Özellik Seviyesi Birleştirme (Feature Level Fusion)

Farklı biyometrilerden elde edilen farklı özellik setlerini tek şablon yaratmak için birleştirilmesidir. Her sensörden yakalanan ham veriden kişiyi benzersiz olarak tanımlayan özellik vektörü oluşturulur. Birden fazla özellik vektörünün birleşmesi ile oluşan tek vektör çok boyutluluk sağlar ve kişinin doğru tanımlanma olasılığı artar. Birleştirilmiş özelliklerin her biri bağımsız ve aynı tür ölçüm türü kullanılmış ise özellik seviyesi birleştirme etkili olarak çalışır. Bu birleştirme her zaman uygulanamaz. Çünkü birbirine uyuşmayan veya farklı benzerlik ölçümü gerektiren yerlerde kullanılmaz (minuatiae set ve textural descriptor parmakizi için). Sorgu vektörü ve Öklid mesafe ölçümü gibi mesafe tabanlı veri tabanı arasında mesafe skoru hesaplanır. Şekil 2'de özellik seviyesi birleştirmenin çalışması genel olarak görülmektedir.



Şekil 2. Özellik Seviyesi Birleştirme

Çoklu özellik setleri, aynı özellik çıkarım algoritmasını kullanarak aynı biyometrinin farklı örnekleri ile uyuştuğunda, özellik seviyesi birleştirme şablon güncellenir. Bu işlem diğer birleştirme tekniklerinden daha doğru sonuç üretmesini sağlar. Özellik seviyesi birleştirmenin zorluğu çeşitli özelliklerin uyuşmaması veya her biri arasındaki yüksek bağımlılıklardır [2-3].

Murakami ve diğerleri sıralı özellik seviyesi birleştirme için biyometrik özellikleri birleştiren ve her seferinde girilen biyometrik örneğe göre kara veren genel framework önermişlerdir. Parmak damar izine bulanık taahhüt ile uyguladıkları yöntemi çeşitli saldırılar ile analiz etmişlerdir [4].

Selwal ve diğerleri, multimodal biyometrik sistemleri için özellik seviyesinde bileştirme yöntemini bulanık ilişkiler işlemi ile gerçekleştirmişlerdir. Geliştridikleri şema EER ve GAR oranlarında kayda değer gelişme olduğunu tespit etmişlerdir [5].

Güvenliği arttırmak için özellik seviyesinde biyometrik veriden çıkarılan özellikleri birleştirerek diğer domaine dönüştürmüşlerdir. Bu sistem ile GAR %100, EER %28 olarak elde edilmiştir [6].

Parmak izi ve parmak damar izi biyometrilerini LDA, CCA, Kernel-CCA, SLPCCA özellik seviyesi birleştirme yöntemlerini, gabor filtresi kullandığı ve en yakın komşu sınıflama yöntemi ile veriyi sınıflandırdıktan sonra karşılaştırmış ve aşağıdaki verileri elde etmiştir [7].

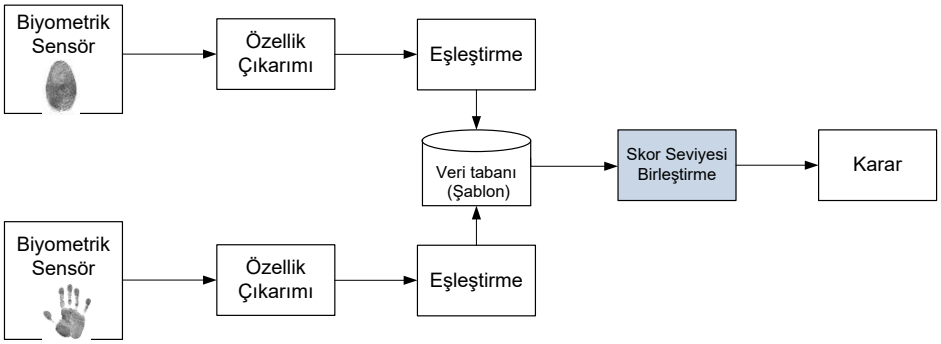
Lu ve Peng çalışmalarında özellik seviyesi birleştirme tekniği ile parmak izi, parmak boğumu, parmak damar ve parmak şekli biyometrik bilgilerini güvenli bir taslakta birleştirip korumayı amaçlamıştır. Çalışmalarının sonucunda çoklu parmak biyometrisinin yüksek doğrulama oranı ve güvenlik seviyesinin yüksek olduğunu tespit etmişlerdir [8].

Gawande ve dig., iris ve parmak izinin özniteliklerini birleştirerek özellik seviyesinde birleştirme alt yapısı geliştirmişlerdir. Mahalanobis mesafe ölçüm yöntemi ile tek biyometrik özellikleri birleştirerek birleşik çoklu model biyometrik şablon elde etmişlerdir. Üretilen birleşik şablonu kullanarak geliştirdikleri yapay sinir ağları temelinde Radyal Temelli fonksiyon ile tanıma işlemini gerçekleştirmiştir ve tek biyometrik veriye göre daha iyi tanıma performansı elde ettiğini belirlemişlerdir. Mahalanobis mesafe tekniği ile FAR %0, FRR %8 tespit edilmiştir [9].

2.3. Eşleştirme Skor Seviyesi Bileştirme (Match Score Level Fusion)

Bu yöntemde, Şekil 3'te görüldüğü gibi aynı veya farklı özellik setine uygulanan birden fazla sınıflandırıcıdan alınan puanlar nihai kararı almak için birleştirilir. Karar seviyesindeki birleştirmeden daha etkili bir yöntemdir. Her bir biyometrik sistem kendi eşleştirme skorunu ölçer ve hesaplar. İki biyometrik veri arasındaki benzerlik derecesi tabanlı eşleştirme skorunun hesaplanmasıdır. Elde edilen skorlar ile tek eşleştirme skoru elde edilir. Eşleştirme skoru benzerlik veya örnekten üretilen özellikler arasındaki mesafenin ölçüsüdür ve şablon olarak saklanır. Eşleşme yada eşleşmeme kararı karar eşik değerine göre belirlenir. Kullanılan

yöntemlerden bazıları min-max, quadratic-line, SVM, Fisher's linear, Bayes sınıflama, karar ağaçları

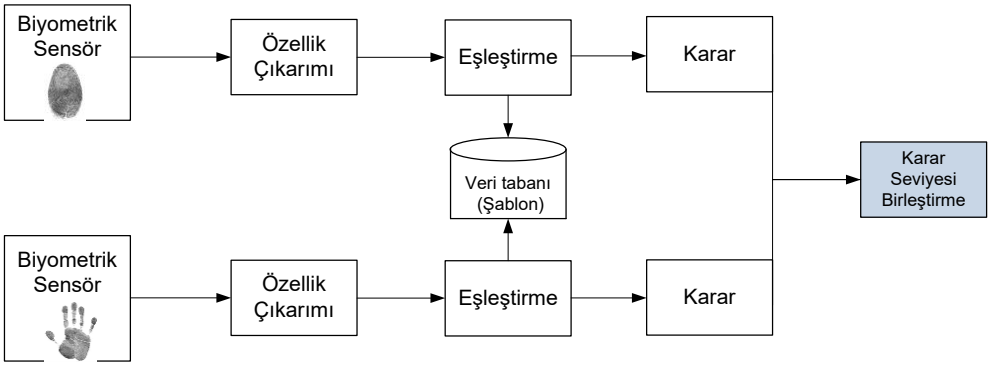


Şekil 3. Eşleştirme Seviyesi Birleştirme

Sim ve diğerleri, Yüz ve iris biyometrilerini kullanarak eşleştirme tabanlı bir sistem geliştirmişlerdir [10].

2.4. Karar Seviyesi Birleştirme (Decision Level Fusion)

Bu, puanların çoğunluk oyu veya diğer füzyon kurallarını kullanarak füzyon öncesinde ikili (eşleşmiş / eşleşmeyen) bir forma dönüştüğü, skor düzeyi füzyonunun özel bir örneği olarak görülebilir. Her biyometrik sistem karar oluşturur ve sonra bu kararlar genellikle çoğunluk oylama şeması kullanılarak Şekil 4'te görüldüğü gibi birleştirilir. Bazı metotlar her biyometrinin kararını ağırlıklandırma ile gerçekleştirir. Karar seviyesi her sınıflandırıcıya "kabul" yada "red" bilgisi sağlar. Bu yaklaşım, farklı biyometrik özellikler arasında en az karmaşıklık ve maksimum birlikte işlerlik gösterir, ancak füzyon aşamasında mevcut sınırlı bilgi miktarı nedeniyle skor seviyesi füzyonundan daha az etkindir.



Şekil 4. Karar Seviyesi Birleştirme

Li ve ark. karar seviyesinde birleştirme tekniği ile parmak izi temelinde çoklu biyometrik şifreleme sistemi geliştirmişlerdir. Sistemde her biyometrik veriyi korumak için kıyım(hash) fonksiyonu uygulanmıştır. Çalışma sonucunda önerilen sistemin tek biyometrik verinin kullanıldığı sistemlere göre daha iyi yetkilendirme gerçekleştirdiği ve daha güçlü güvenlik sağladığı tespit edilmiştir [11].

2.5. Hibrid Birleştirme (Hybrid Fusion)

Çeşitli birleştirme seviyelerinin bir arada kullanılmasıdır. Eskandari ve Toygar, en etkili yüz ve iris biyometrik kodu elde etmek için global ve yerel özellik çıkarım metotları ile yüz ve iris biyometrilerini skor ve özellik seviyesi füzyon tabanında birleştiren yeni şema önermişlerdir. Özellik seviyesinde özellikleri azaltmak ve skor seviyesinde ağırlıkları optimize etmek için BSA ve PSO yöntemleri şemada kullanılmıştır [12].

Sharifi ve Eskandari, skor, özellik ve karar seviye füzyonları, yüz ve iris biyometrilerini Log-Gabor filtresi ile özelliklerini çıkararak etkili bir şekilde birleştirmeye çalışmışlardır. Tanıma doğruluğunu arttırmak için BSA algoritması ile özellik sayısı azaltılmış ve özellik ve skor seviyesi için en iyi ağırlıklar seçilmiştir. Çalışma sonucunda doğrulama performasının arttığı belirlenmiştir [13].

Parmakizi ve parmak damar izinden Gabor filtresi ile özellikleri çıkartmışlardır. PCA ve Kernel PCA kullanarak özellikleri seçilmiş ve KNN, Naive Bayes ve RBF yapay sinir ağı ile sınıflandırma yapılmıştır. Çalışma sonucunda Kernel PCA ile RBF sınıflayıcı yönteminin diğer yöntemlerden daha başarılı sonuç verdiği belirlenmiştir [14].

Yüz ve kulak biyometrisindeki benzerlikleri kullanarak birleştirilmiş çoklu biyometrik şablon koruma yöntemini Yuan ve Li bir çalışmalarında önermiştir. Önerdikleri yöntemde ilk olarak yüz ve kulak vektörlerini özellik seviyesinde birleştirilmiş, ikinci olarak ise birleştirilen özelliklere geri dönüşümsüz bir fonksiyon uygulanmıştır. Daha sonra dönüştürülen şablonu korumak için Bulanık Kasa yöntemi kullanılmıştır. Sistem: görüntünün ön işlenmesi, Gabor-PCA ile özellik çıkarımı, özellik seviyesi birleştirme, şablon dönüşümü, birleştirilmiş şablon şifrelemesi, birleştirilmiş şablon deşifrelemesi aşamalarında oluşmaktadır [15].

3. SONUÇ VE TARTIŞMA (CONCULUSION AND DISCUSSION)

Biyometrik sistemlerde doğru kişiyi tanıma önemli bir konudur. Bu nedenle tek biyometrik özellik yerine birden fazla biyometrik özellik kullanılması tanıma performansını arttıracaktır. Biyometrik bilgilerden elde edilen şablonlar güvenlik açısından ayrı ayrı tutulmak yerine tek şablon olarak tutulması daha güvenilir olmaktadır. Biyometrik şablonların tek şablon olarak birleştirilmesi için çeşitli yöntemler geliştirilmiştir. Bu yöntemlerin kendilerine göre avantaj ve dezavantajları bulunmaktadır.

Sensör ve özellik seviyesi birleştirme yöntemleri biyometrik hakkında fazla bilgi sunar ama yüksek hesaplama gerektirmektedir. Eşleştirme seviyesi birleştirme ise özet seviyede bilgi sunar ve ayrıca daha az hesaplama gerektirir. Özellik seviyesi füzyonu, artan karmaşıklıkla eşleştirme skoru seviyesi füzyonundan daha iyi performans göstermektedir. Aynı zamanda özellik seviyesi birleştirme şablonların özelliklerini birleştirmekte bu yüzden kişi tanımada daha fazla doğruluk oranı sağlamaktadır. Eşleştirme seviyesi ise şablondaki verilerin sınıflandırmasına dayanmaktadır. Biyometrik veriler arasındaki benzerliklerden elde edilen skorların sınıflandırılmasıdır. Özellik seviyesi ve eşleştirme seviyelerinin başarı seviyeleri yüksektir. Bu iki füzyon seviyesinin birleşimi daha yüksek tanıma performansı sağlayacaktır.

Birleştirme yöntemleri arasındaki farktan dolayı yetkilendirme sistemlerinde en uygun yöntemin seçilerek tanıma performansının arttırılması gereklidir. Böylece füzyon türünü seçmek çalışılan kaynak, uygulama ve güvenlik seviyesini etkilediğinden önem kazanmaktadır. Uygun özellik çıkarım tekniği seçimi ve en uygun füzyon seviyesi seçimi çoklu biyometrik sistem kurulumunda çözülmesi gereken konulardan biridir.

4. KAYNAKLAR (REFERENCES)

[1]. Nagar, A., Nandakumar, K., & Jain, A. K. (2012). Technical Report: Multibiometric Cryptosystems. *Under review for IEEE TIFTS*, *7*(1).

[2]. A. Ross and A. Jain, (2003). "Information Fusion in Biometric," *Journal of Pattern Recogniton Letters*, pp. 2115-2125.

[3]. Rattani A. and Tistarelli M., (2009). "Robust multimodal and multiunit feature level fusion of face and iris biometrics," *International conference of biometrics*, pp. 960-969.

[4]. Murakami T., Ohki T., and Takahashi K., (2016). "Optimal sequential fusion for multibiometric cryptosystems," *Information Fusion32*, pp. 93-108.

[5]. Selwal A., Gupta S., and Kumar S., (2016). "A scheme for template security at feature fusion level in multimodal biometric system," *Advances in Science and technology* , pp. 23-30.

[6]. Patel H., Panuvala C., and Vora A., (2016). "Hybrid feature level approach for multi-biometric cryptosystem," *IEE Wispnet 2016*, pp. 1087-1092.

[7]. Yang J. and Zhang X., (2012). "Feature-level fusion of fingerprint and finger-vein for personal identification," *Pattern Recognition Letters 33 (2012)* , p. 623–628.

[8]. Lu L. and Peng J., (2014). "Finger multi-biometric cryptosystem using feature-level fusion," *Inetrnational journal of signal processing and pattern recognition 7*, pp. 223-235.

[9]. Gawande U., Zaveri M., and Kapur A., (2013). "Fingerprint and iris fusion based recognition using rbf neural network," *Journal of signal and image processing 4*, pp. 142-148.

[10]. Sim H., Asmuni H., Hassan R., and Othman R., (2014). "Multimodal biometrics: Weighted score level fusion based on non-ideal iris and face images," *Expert Systems with Applications*, pp. 5390-5404.

[11]. Li C., Hu J., Pieprzyk J., and Susilo W., (2015). "A new bioceyptosystem-oriented security analysis framework and implemantation of multibiometric cryptosystems based on decision level fusion," *IEE transaction on information forensics and security 10*, pp. 1193-1206.

[12]. Eskandari M. and Toygar Ö., (2015). "Selection of optimized features and weights on face-iris fusion using distance images," *Computer Vision and Image Understanding*, pp. 63-75.

[13]. Sharifi O. and Eskandari M., (2016). "Optimal Face-Iris Multimodal Fusion Scheme," *Symmetry 2016*, pp. 1-16.

[14]. Viswanathan A. and Chitra S., (2014). "Multimodal Biometrics Based on Fingerprint and Finger Vein," *Journal of Applied Sciences, Engineering and Technology 8(2)*, pp. 226-234.

[15]. Yuan L. and Li W., (2015). "Multimodal Template Protection Based on Data Transformation and Fuzzy Vault ," *Journal of Computational Information Systems 11: 11 (2015)* , p. 3999–4008.