

Makine Öğrenimi Modellerini Kullanan EMG Tabanlı Biyometrik Yaklaşımlar: Kısa Derleme

Kutlucan Görür^{1,*}, İlyas Özer², Onursal Çetin¹, Feyzullah Temurtas¹

¹Bandırma Onyedi Eylül Üniversitesi, Elektrik-Elektronik Mühendisliği

²Bandırma Onyedi Eylül Üniversitesi, Bilgisayar Mühendisliği

*kgorur@bandirma.edu.tr

Biyometrik tanıma sistemleri, bir bireyi vücudunun benzersiz özelliklerine göre tanıyan bir teknoloji sunar. Bu teknoloji, bir kişinin fiziksel özelliklerini analiz ederek ve veri tabanında depolanan ana bilgisayar verileriyle eşleşip eşleşmediğini belirleyerek ana bilgisayarın kimliğini doğrulamaktadır. Örneğin, kimlik doğrulama sistemleri, parmak izi veya iris deseni veya ana bilgisayarın yüz şekli gibi özellikleri analiz eder. Bununla beraber kullanıcının akıllı telefonuna entegre edilmiş bir ivmeölçer kullanılarak yürüyüşü analiz edilerek veya sesin karakteristik frekansı analiz edilerek bir kişinin kimliği doğrulanabilmektedir. Son yıllardaki en umut verici biyometrik teknoloji, elektromiyogram (EMG) sinyalleri gibi kas hareketi sinyalinin kullanılmasıdır. Bu yöntem, EMG sinyallerinin morfolojik özelliklerini analiz ederek gerçek zamanlı kimlik doğrulamayı sağlamaktadır. Böylece bilgisayar korsanlığı gibi durumları önlediği için biyometrik teknoloji alanında önemli bir gelişme potansiyeline sahiptir. Bu literatür özetinde EMG tabanlı biyometrik çalışmalar anlatılmıştır.

Anahtar kelimeler: EMG, Biyometrik, Makine Öğrenmesi, Derleme

© 2022 Published by AInteliala

EMG-based Biometric Approaches using Machine Learning Models: A Concise Survey

Kutlucan Görür^{1,*}, İlyas Özer², Onursal Çetin¹, Feyzullah Temurtas¹

¹Bandırma Onyedi Eylül University, Electrical and Electronics Department

²Bandırma Onyedi Eylül University, Computer Engineering Department

*kgorur@bandirma.edu.tr

Biometric recognition systems offer technology that recognizes an individual based on their body's unique characteristics. This technology verifies the identity of the host by analyzing a person's physical characteristics and determining if they match the host data stored in the database. For example, authentication systems analyze features such as fingerprint or iris pattern, or host's face shape. However, a person's identity can be verified by analyzing the gait or the characteristic frequency of the sound using an accelerometer integrated in the user's smartphone. The most promising biometric technology in recent years is the use of unique signals such as electromyogram (EMG). This method provides real-time authentication by analyzing the morphological features of EMG signals. Thus, it has a significant development potential in the field of biometric technology, as it prevents hacking. In this literature summary, EMG-based biometric studies are described.

Keywords: EMG, Biometric, Machine Learning, Survey

1. Giriş

ATM'ler, cep telefonlarına erişim, güvenli ödeme ve hatta askeri silah kullanma izni gibi çok çeşitli uygulama senaryolarında güvenli kullanıcı kimlik doğrulama sistemlerine olan talep hızla artmaktadır [1]. Kullanıcı doğrulama yaklaşımları, “kullanıcının ne bildiği” (şifreler gibi), “kullanıcının sahip olduğu” (kimlik kartları gibi) ve “kullanıcının ne olduğu” (biyometri gibi) olmak üzere üç kategoriye ayrılabilir. Ancak, bu üç yaklaşımın her birinin kendi sınırlamaları vardır. Mesela parolalar, güvenlik kameraları tarafından kolayca çalınabilir. Kimlik kartları da kazara kaybolabilir veya kasıtlı olarak çalınabilir. Ayrıca, her zaman bir kimlik kartı taşımak sakıncalıdır [1]. DNA, insan yüzü, parmak izi, iris ve fizyolojik sinyaller gibi biyometrik yaklaşımlar, bir dereceye kadar yukarıdaki yaklaşımların dezavantajlarını telafi edebilir. Bununla birlikte, mevcut biyometrik yöntemlerin hepsinin dezavantajları vardır. DNA, tükürük ve saç dökülmesi yoluyla kolayca çalınır. Derinlik fotoğrafçılığı ile yüz ve iris yakalanabilir. Parmak izleri, dokunulan herhangi bir yüzeyden alınabilir ve plastik kalıplarla dövülebilir. Daha da kötüsü, mevcut tüm biyometrik tabanlı şifreler iptal edilemez [1]. Diğer bir deyişle, DNA, yüz, iris veya parmak izlerinden alınan bilgiler çalınırsa, kullanıcı bunları kendi isteğiyle değiştiremez. Ek olarak, kullanıcılar aynı biyometriyi farklı uygulamalarda kullanabilirler. Bir uygulamadaki biyometrik şablon çalınırsa, iptal edilemezlik nedeniyle diğer tüm uygulamalardakiler tehlikeye girer. Öte yandan, elektroensefalogram (EEG) ve elektrokardiyogram (EKG) gibi fizyolojik sinyallere dayanan yeni biyometrik yaklaşımlar, çalınmaları veya taklit edilmeleri zor olduğu için büyük umut vaat etmektedir [1]–[3]. Ancak, kullanıcı kimlik doğrulama doğruluğu şu anda pratik uygulamalarını desteklemek için çok düşüktür [1].

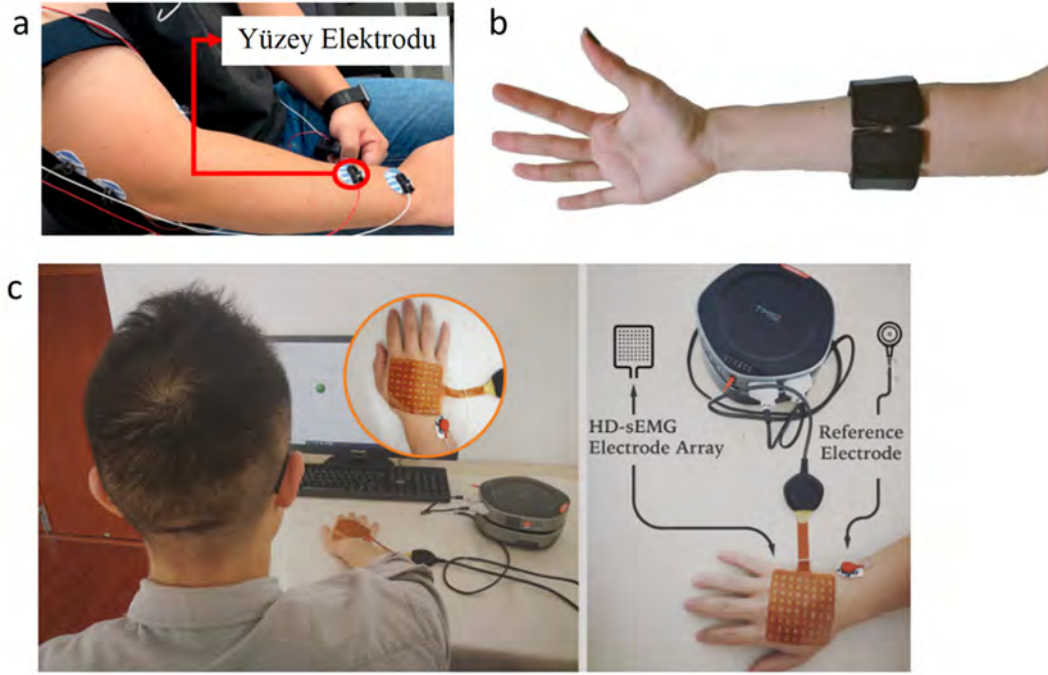
Buna karşılık, yüzey elektromiyogramı (sEMG), çok kullanıcıli miyoelektrik arayüz tekniklerinde denekler arasında farklı özellikler göstermiştir. Bu özellik, sEMG'nin yeni bir biyometrik modalite olarak kullanılabilmesini gösterir. EEG tabanlı biyometrik yaklaşım ile karşılaştırıldığında, sEMG sinyalinin toplanması daha uygundur. Ayrıca, sEMG sinyal özellikleri, farklı kas kasılma modellerine göre değişir ve ikinci bir şifrelemeye izin verir; bu, güç uygulamak için benzersiz bir model tasarlayarak bulunan ilk şifrelemenin ötesindedir [1]–[3]. Şimdiye kadar, çok az çalışma bir kimlik doğrulama yöntemi olarak sEMG'nin uygulanabilirliğini araştırdı. Önceki çalışmaların bazılarında biyometri, olarak belirli el hareketleri altında sEMG kullanılmıştır. sEMG sinyallerinin diğer uygulamaları, yalnızca biyometrik yaklaşımların tamamlayıcısı olarak araştırılmıştır (örneğin, ECG ve tuş vuruşu dinamikleri) [1]–[3]. Genel olarak farklı günlerdeki sinyal değişkenliği dikkate alınmamıştır. Eğitim ve test verileri farklı günlerde kaydedilmemiştir. Bu açıdan farklı gün ve denemelerde EMG ölçümünün güvenilir bir biyometrik sistem tasarlamak bakımından önemli olduğu literatürde belirtilmiştir [1]–[3].

EMG sinyali, bir kas kasılması olduğunda üretilen bir mikro akımı ölçerek voltaj değeri şeklinde elde edilen bir sinyali temsil eder. EMG sinyallerini ölçmenin iki yöntemi vardır: iğne elektrot yöntemi ve yüzey elektrot yöntemi. İğne elektrot yöntemi, kas içine bir iğne elektrotu sokarak kasın bir noktasında oluşan aksiyon potansiyelini ölçer. Yüzey elektrot yöntemi, elektrotları cilt yüzeyine yerleştirilerek bir aksiyon potansiyelini ölçer. Elektrot yerleştirme pozisyonu açısından, sinyal, elektrotun deney sırasında değişen bir kasa veya mevcut çalışmalarda sıklıkla kullanılan bir kas pozisyonuna yerleştirilmesiyle ölçülür [1]–[3].

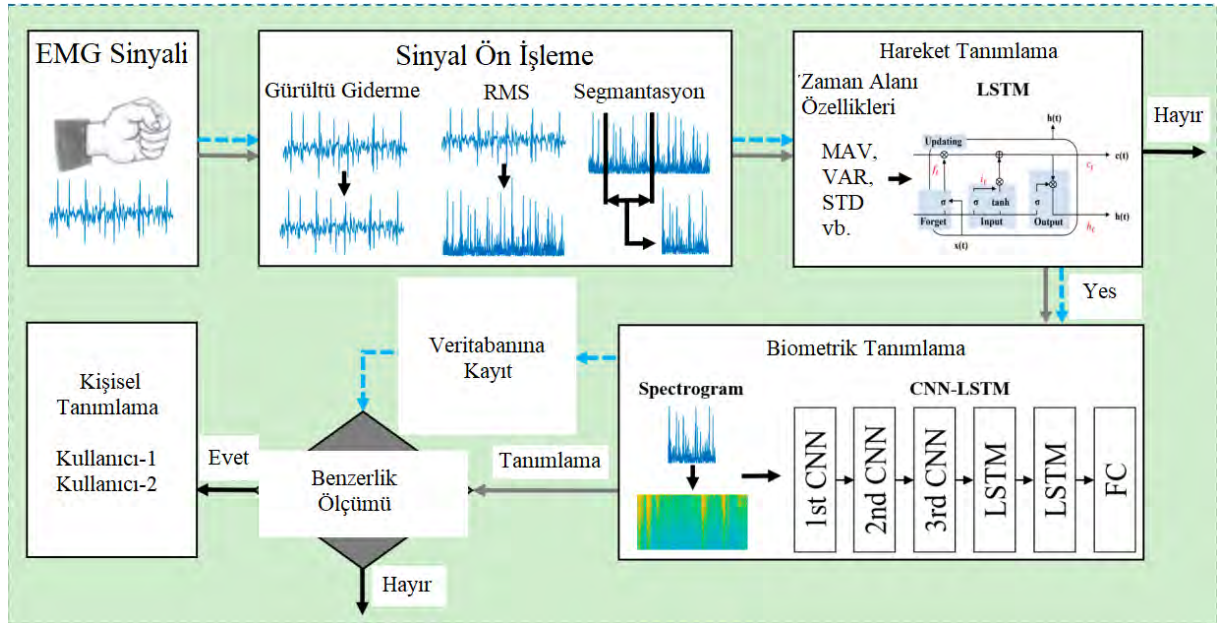
Makine öğrenimi teknolojisi, modern toplumun birçok yönüne güç vermektedir. Web aramalarından sosyal ağlarda içerik filtrelemeye, e-ticaret web sitelerindeki önerilerden, kameralar ve akıllı telefonlar gibi tüketici ürünlerinde giderek daha fazla yer almaktadır Makine öğrenimi sistemleri, görüntülerdeki nesneleri tanımlamak, konuşmayı metne dönüştürmek, haber öğelerini, gönderileri veya ürünleri kullanıcıların ilgi alanlarına göre eşleştirmek ve ilgili arama sonuçlarını seçmek için kullanılır. Giderek, bu uygulamalar derin öğrenme adı verilen makine öğrenmesi modellerini kullanmaktadır. Biyolojik sinyal örüntü tanıma ve biyometrik yaklaşımlarda da son yıllarda en çok kullanılan makine öğrenmesi modellerinin derin öğrenme modelleri olduğunu görmekteyiz [4]. İlgili bu literatür özeti çalışmasında da makine öğrenmesi modelleri ve diğer sinyal işleme yöntemlerini kullanan EMG tabanlı biyometrik yaklaşımlar ele alınmıştır.

2. Sinyal Elde Etme ve Metotlar

EMG tabanlı biyometrik yaklaşımlarda sinyal işleme ve makine öğrenmesi algoritmaları kullanılmaktadır. Buna göre izlenen örüntü tanıma adımları farklı kişileri ayırt edebilmektedir. EMG sinyallerinin elde edilmesi için çok kanallı ve/veya tek kanallı yüzey elektrotları kullanılmaktadır (bakınız Şekil 1) [2]. Biyometrik örüntü tanıma için uygulanan sinyal işleme adımları da Şekil 2’de gösterilmektedir.



Şekil 1. Biyometrik yaklaşımlar için farklı bölgelerden ve farklı kanallarda EMG sinyali elde edilmesi a- [2] b- [3] c- [1]



Şekil 2. EMG tabanlı biyometrik yaklaşıma ait sinyal işleme ve makine öğrenmesi adımları [2]

Biometrik sinyaller üzerinden örüntü tanıma işleminde son yıllarda ön plana çıkan makine öğrenmesi yöntemi derin öğrenme olarak literatürde görülmektedir. Derin öğrenme, birden çok işleme katmanından oluşan hesaplama modellerinin, birden çok soyutlama düzeyiyle verilerin temsillerini öğrenmesine olanak tanır. Bu yöntemler, konuşma tanıma, görsel nesne tanıma, nesne algılama ve ilaç keşfi ve genomik gibi diğer birçok alanda en son teknolojiyi önemli ölçüde geliştirmiştir. Derin öğrenme, bir makinenin önceki katmandaki temsilden her katmandaki temsili hesaplamak için kullanılan dahili parametrelerini nasıl değiştirmesi gerektiğini belirtmek için geri yayılım algoritmasını kullanarak büyük veri kümelerinde

karmaşık yapıyı keşfeder. Derin kıvrımlı ağlar görüntü, video, konuşma ve ses işlemede çığır açarken, tekrarlayan ağlar metin ve konuşma gibi sıralı verilere ışık tutmuştur [4].

3. Literatür Özeti

EMG tabanlı biometrik yaklaşımlara ait kısa literatür özeti Tablo 1’de görülmektedir. Buna göre EMG tabanlı biometrik yaklaşımlarda kanal sayısının önemli olduğu ve kullanım kolaylığı sağladığı belirtilmektedir. Özellik çıkarma ve makine öğrenmesi yöntemleri de biometrik örüntü tanıma da biometrik sistemin başarısını değiştirmektedir.

Tablo 1. EMG tabanlı biometrik sistemlere ait kısa literatür özeti

Çalışmalar	Sinyal	Kanal Sayısı	Özellik Çıkarma Yöntemi	Makine Öğrenmesi Yöntemi
[5]	EMG	8	PCA	ED, KNN, SVM
[6]	EMG	2	VAR, Mean Length, ZC, MF	ANN, SVM, KNN
[7]	EMG	8	CWT, CNN	CNN
[8]	EMG	8	CNN	CNN
[9]	EMG	11	RMS, MAV, vb.	LDA
[10]	EMG	3	CNN	CNN
[3]	EMG	8	DWT, CWT, RMS vb.	CNN, ExtraTrees
[11]	EMG	1	MAV, VAR, RMS vb.	OCSVM, LOF
[12]	EMG	2	ZC, MF, vb.	SVM
[13]	ECG, EMG	1	AC, FFT	OPF

4. Sonuç

EMG tabanlı biometrik yaklaşımlar son yıllarda ön plana çıkmaktadır. Bu sinyallerin diğer EEG ve ECG gibi sinyallere göre kolay toplanması ve frekans bant aralığının geniş olması biometrik yaklaşımlar açısından avantaj olarak görülmektedir. Özellikle MYO kol-bantı gibi çok kanallı ve kablolu olarak toplanan EMG tabanlı biometrik yaklaşımlar ile tek-kanallı olarak toplanabilen biometrik sistemlerin ön plana çıkması ve gerçek-zamanlı birçok uygulama alanı bulabileceği görülmektedir.

Referanslar

- [1] X. Jiang *et al.*, “Neuromuscular Password-Based User Authentication,” *IEEE Trans. Ind. Informatics*, vol. 17, no. 4, pp. 2641–2652, Apr. 2021, doi: 10.1109/TII.2020.3001612.
- [2] J.-S. Kim, M.-G. Kim, and S.-B. Pan, “Two-Step Biometrics Using Electromyogram Signal Based on Convolutional Neural Network-Long Short-Term Memory Networks,” *Appl. Sci.*, vol. 11, no. 15, p. 6824, Jul. 2021, doi: 10.3390/app11156824.
- [3] L. Lu, J. Mao, W. Wang, G. Ding, and Z. Zhang, “A Study of Personal Recognition Method Based on EMG Signal,” *IEEE Trans. Biomed. Circuits Syst.*, vol. 14, no. 4, pp. 681–691, Aug. 2020, doi: 10.1109/TBCAS.2020.3005148.
- [4] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/nature14539.
- [5] S. Venugopalan, F. Juefei-Xu, B. Cowley, and M. Savvides, “Electromyograph and keystroke dynamics for spoof-resistant biometric authentication,” in *2015 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Jun. 2015, pp. 109–118, doi: 10.1109/CVPRW.2015.7301326.
- [6] S. Shin, J. Jung, and Y. T. Kim, “A study of an EMG-based authentication algorithm using an artificial neural

network,” in *2017 IEEE SENSORS*, Oct. 2017, pp. 1–3, doi: 10.1109/ICSENS.2017.8234158.

- [7] L. Lu, J. Mao, W. Wang, G. Ding, and Z. Zhang, “An EMG-Based Personal Identification Method Using Continuous Wavelet Transform and Convolutional Neural Networks,” in *2019 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, Oct. 2019, pp. 1–4, doi: 10.1109/BIOCAS.2019.8919230.
- [8] R. Shioji, S. Ito, M. Ito, and M. Fukumi, “Personal Authentication and Hand Motion Recognition based on Wrist EMG Analysis by a Convolutional Neural Network,” in *2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS)*, Nov. 2018, pp. 184–188, doi: 10.1109/IOTAIS.2018.8600826.
- [9] M. Lee, J. Ryu, and I. Youn, “Biometric personal identification based on gait analysis using surface EMG signals,” in *2017 2nd IEEE International Conference on Computational Intelligence and Applications (ICCIA)*, Sep. 2017, pp. 318–321, doi: 10.1109/CIAPP.2017.8167230.
- [10] S. Morikawa, S. Ito, M. Ito, and M. Fukumi, “Personal Authentication by Lips EMG Using Dry Electrode and CNN,” in *2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS)*, Nov. 2018, pp. 180–183, doi: 10.1109/IOTAIS.2018.8600859.
- [11] Q. Li, P. Dong, and J. Zheng, “Enhancing the Security of Pattern Unlock with Surface EMG-Based Biometrics,” *Appl. Sci.*, vol. 10, no. 2, p. 541, Jan. 2020, doi: 10.3390/app10020541.
- [12] M. U. Khan, Z. A. Choudry, S. Aziz, S. Z. H. Naqvi, A. Aymin, and M. A. Imtiaz, “Biometric Authentication based on EMG Signals of Speech,” in *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, Jun. 2020, pp. 1–5, doi: 10.1109/ICECCE49384.2020.9179354.
- [13] N. Belgacem, R. Fournier, A. Nait-Ali, and F. Bereksi-Reguig, “A Novel Biometric Authentication Approach using ECG and EMG signals,” *J. Med. Eng. Technol.*, vol. 39, no. 4, pp. 226–238, May 2015, doi: 10.3109/03091902.2015.1021429.