BİLGİSAYAR BİLİMLERİ VE MÜHENDİSLİĞİ ALANINDA BİLİMSEL ARAŞTIRMALAR

Editör: Dr.Öğr.Üyesi Funda AKAR

yaz
yayınları

Bilgisayar Bilimleri ve Mühendisliği Alanında Bilimsel Araştırmalar

Editör

Dr.Öğr.Üyesi Funda AKAR

yaz yayınları

2026

yaz
yayınları

Bilgisayar Bilimleri ve Mühendisliği Alanında Bilimsel Araştırmalar

Editör: Dr.Öğr.Üyesi Funda AKAR

E_ISBN 978-625-8574-69-2

Mart 2026 – Afyonkarahisar

Dizgi/Mizanpaj: YAZ Yayınları

Kapak Tasarım: YAZ Yayınları

YAZ Yayınları. Yayıncı Sertifika No: 73086

M.İhtisas OSB Mah. 4A Cad. No:3/3
İscehisar/AFYONKARAHİSAR

www.yazyayinlari.com

yazyayinlari@gmail.com

İÇİNDEKİLER

FPGA VE DONANIM TABANLI SİSTEMLERDE FİKRİ MÜLKİYET KORUMASI: DONANIM GÜVENLİĞİ PERSPEKTİFİ

Sezen BAL[1]

1. GİRİŞ

Yarı iletken teknolojilerindeki gelişmeler, elektronik sistemlerin işlevsel yoğunluğunu ve ekonomik değerini artırırken donanım güvenliği ile fikri mülkiyet korumasını da temel bir araştırma ve uygulama alanı haline getirmiştir. Alanda programlanabilir kapı dizileri (Field Programmable Gate Array, FPGA), uygulamaya özel tümdevreler (Application-Specific Integrated Circuit, ASIC) ve yonga üzeri sistemler (System-on-Chip, SoC), haberleşme, savunma, otomotiv, sağlık, endüstriyel otomasyon ve nesnelerin interneti gibi birçok kritik alanda kullanılmaktadır. Bu platformlarda yer alan donanım fikri mülkiyet blokları, yüksek geliştirme maliyetleri ve yeniden kullanılabilir yapıları nedeniyle önemli bir teknik ve ekonomik değere sahiptir (Pilato, 2022; Rajendran, 2017; Anshul ve Sengupta, 2024).

Modern donanım tasarım ekosistemi, çok aktörlü ve küresel ölçekte dağılmış bir tedarik zinciri yapısına sahiptir. Gereksinim tanımlama, tasarım, sentez, netlist üretimi, üretim, test, paketleme ve dağıtım aşamalarında farklı tarafların yer alması, donanım fikri mülkiyetinin gizliliği ve bütünlüğü açısından ek riskler doğurmaktadır. Özellikle üçüncü taraf fikri mülkiyet kullanımı, dış kaynaklı üretim ve karmaşık tasarım

[1] Doktor Öğretim Üyesi, Marmara Üniversitesi, Teknik Bilimler Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, ORCID: 0000-0002-7244-6613.

araçları, tasarım sırlarının açığa çıkması veya yetkisiz kullanım olasılığını artırmaktadır (Bhunia ve ark., 2022; Hu ve ark., 2020; Akter ve ark., 2023).

Yazılım güvenliğinden farklı olarak donanım güvenliği, tasarımın fiziksel gerçeklemesiyle doğrudan ilişkilidir. Bu nedenle tersine mühendislik, klonlama, sahtecilik, fazla üretim, donanım truva atı, yan kanal analizi ve yetkisiz yeniden yapılandırma gibi tehditler yalnızca işlevsel doğruluğu değil, tasarımın sahipliğini ve güvenilirliğini de hedef almaktadır (Hu ve ark., 2020; Akter ve ark., 2023; Guin ve ark., 2014). FPGA tabanlı sistemlerde ise bit akışı güvenliği, anahtar yönetimi ve hata ayıklama arayüzleri özel önem taşımaktadır (Açar ve ark., 2025).

Bu bölümde FPGA ve donanım tabanlı sistemlerde fikri mülkiyet koruması donanım güvenliği perspektifinden ele alınmaktadır. Öncelikle kavramsal temel ortaya konmakta, ardından tasarım yaşam döngüsündeki güvenlik açıkları, başlıca tehditler ve koruma yöntemleri değerlendirilmektedir. Devamında FPGA'ye özgü güvenlik mekanizmaları, güvenlik-performans-maliyet ilişkisi ve güncel yönelimler tartışılmaktadır.

2. DONANIM GÜVENLİĞİ VE FİKRİ MÜLKİYET KORUMASININ TEMELLERİ

Donanım güvenliği, bir elektronik sistemin yalnızca doğru çalışmasını değil, aynı zamanda tasarım bilgilerinin, işlevsel bütünlüğünün ve kullanım yetkisinin korunmasını amaçlayan çok katmanlı bir güvenlik alanıdır. Bu alan, tasarım aşamasından üretime ve saha kullanımına kadar uzanan süreçte gizlilik, bütünlük, erişim denetimi ve güvenilirlik gereksinimlerini kapsamaktadır. Dolayısıyla donanım güvenliği yalnızca fiziksel koruma ya da saldırı tespiti ile sınırlı değildir. Yaşam döngüsü boyunca ortaya çıkabilecek tehditlere karşı sistematik savunma

mekanizmalarının geliştirilmesini de içermektedir (Hu ve ark., 2020; Akter ve ark., 2023).

Bu çerçevede donanım fikri mülkiyeti (Intellectual Property, IP), belirli bir işlevi yerine getirmek üzere geliştirilen ve farklı tasarımlarda yeniden kullanılabilen modüler donanım bileşenlerini ifade etmektedir. İşlemci çekirdekleri, kriptografik modüller, bellek denetleyicileri, haberleşme arabirimleri ve sayısal işaret işleme birimleri bu kapsamdaki başlıca örneklerdir. Yeniden kullanılabilir IP blokları, geliştirme süresini ve maliyeti azalttıkları için özellikle SoC ve FPGA tabanlı sistemlerde yaygın biçimde tercih edilmektedir. Ancak bu özellik, IP'nin ekonomik değerini artırdığı kadar izinsiz çoğaltma, tersine mühendislik, korsan kullanım ve sahte sahiplik iddiası gibi riskleri de beraberinde getirmektedir (Pilato, 2022; Rajendran, 2017).

Bu nedenle fikri mülkiyet koruması, yalnızca geliştiricinin ekonomik haklarını savunmaya hizmet etmemektedir. Aynı zamanda güvenilir bir tedarik zinciri kurulmasına, sahte ya da değiştirilmiş bileşenlerin sisteme sızmasının engellenmesine ve sistem güvenilirliğinin korunmasına da katkı sağlamaktadır. Özellikle üçüncü taraf IP kullanımının yaygın olduğu tasarımlarda, koruma mekanizmalarının doğrudan tasarımın içine yerleştirilmesi gerekli hale gelmektedir (Bhunia ve ark., 2022; Shamsi ve ark., 2019).

Donanım güvenliği ile yazılım güvenliği arasındaki temel fark, tehditlerin büyük ölçüde fiziksel gerçeklemede ortaya çıkması ve sonradan düzeltilmesinin daha güç olmasıdır. Yazılım açıkları çoğu zaman güncellemelerle giderilebilirken, donanım düzeyindeki zafiyetler üretim sonrasında kalıcı sonuçlar doğurabilmektedir. Ayrıca donanım bileşenleri tersine mühendislik, yan kanal gözlemi ve hata enjeksiyonu gibi doğrudan fiziksel saldırılara açık olduğundan, güvenlik yalnızca

mantıksal doğrulukla değil fiziksel davranışla da ilişkilidir (Hu ve ark., 2020; Akter ve ark., 2023).

Donanım IP koruma yöntemleri genel olarak iki amaç etrafında toplanmaktadır. İlki, sahiplik ve aidiyetin ispatlanmasıdır. Filigranlama, parmak izleme, sayısal imza ve steganografi gibi yöntemler bu grupta yer almakta ve korsan kullanım sonrasında hak sahibinin belirlenmesini kolaylaştırmaktadır. İkincisi ise önleyici korumadır. Gizleme, mantıksal kilitleme, kayıt aktarım düzeyi kilitleme ve kamuflajlama gibi yöntemler bu amaçla geliştirilmiş olup, tasarımın anlaşılmasını veya yetkisiz kullanımını zorlaştırmayı hedeflemektedir (Koushanfar ve ark., 2005; Yasin ve ark., 2016; Anshul ve Sengupta, 2024).

FPGA tabanlı sistemler bu genel çerçeve içinde ayrıca önem taşımaktadır. Yeniden yapılandırılabilir yapıları önemli esneklik sağlarken, bit akışının ele geçirilmesi, değiştirilmesi veya analiz edilmesi gibi riskler nedeniyle yeni saldırı yüzeyleri de oluşturmaktadır. Bu nedenle FPGA güvenliği, yalnızca cihazın sunduğu yerleşik güvenlik özellikleriyle değil, tasarım düzeyinde uygulanan IP koruma yöntemleriyle birlikte değerlendirilmelidir.

3. DONANIM TASARIM YAŞAM DÖNGÜSÜNDE GÜVENLİK AÇIKLARI VE TEHDİT MODELİ

Donanım tabanlı sistemlerde güvenlik açıkları yalnızca nihai ürün aşamasında ortaya çıkmamaktadır. Tasarım yaşam döngüsünün hemen her adımında farklı riskler oluşabilmektedir. Sistem gereksinimlerinin belirlenmesi, yüksek seviyeli sentez, kayıt aktarım düzeyi geliştirme, sentez, netlist üretimi, üretim, test, paketleme ve saha kullanımı farklı aktörlerin yer aldığı ve farklı saldırı yüzeyleri barındıran süreçlerdir. Bu nedenle donanım fikri mülkiyetinin korunması, ürün sonrasında eklenen tekil bir önlem olarak değil, yaşam döngüsü boyunca sürdürülen

tehdit odaklı bir güvenlik yaklaşımı olarak ele alınmalıdır (Anshul ve Sengupta, 2024; Bhunia ve ark., 2022).

İlk kritik aşama, spesifikasyon ve mimari tasarımdır. Bu aşamada güvenlik gereksinimlerinin eksik tanımlanması, daha sonra uygulanacak koruma tekniklerinin etkisini doğrudan zayıflatmaktadır. Hangi varlıkların korunacağı, hangi saldırgan modelinin esas alınacağı ve hangi bileşenlerin güven kökü olarak kabul edileceği açık biçimde belirlenmediğinde, sistem işlevsel olarak doğru olsa bile fikri mülkiyet açısından savunmasız kalabilmektedir. Özellikle üçüncü taraf IP kullanımının planlandığı tasarımlarda bu zafiyet daha belirgin hale gelebilmekedir (Pilato, 2022; Akter ve ark., 2023).

Yüksek seviyeli sentez, kayıt aktarım düzeyi geliştirme ve netlist üretimi aşamaları da doğrudan fikri mülkiyet değeri taşımaktadır. Kaynak kod, ara gösterimler ve sentez çıktıları tasarımın işlevsel ve yapısal özelliklerini içerdiği için gizlilik ihlalleri, izinsiz kopyalama ve tersine mühendislik açısından yüksek risk oluşturmaktadır. Özellikle yüksek seviyeli sentez temelli akışlarda güvenlik kısıtları tasarıma gömülebilse de, araç zinciri güvenilmeyen bileşenler içeriyorsa aynı süreç saldırı yüzeyine dönüşebilir (Anshul ve Sengupta, 2024; Pilato, 2022).

Üçüncü taraf IP entegrasyonu, modern SoC ve FPGA tasarımlarının en önemli kırılma noktalarından biridir. Dışarıdan sağlanan bir IP bloğu geliştirme süresini kısaltırken, sistem içine kötü niyetli mantık, arka kapı veya lisans dışı işlevler taşıyabilmektedir. Ayrıca IP sağlayıcısı ile sistem bütünleştiricisi arasında oluşan güven boşlukları, sahte sahiplik iddiası ve yetkisiz yeniden kullanım gibi sorunlara yol açabilmektedir. Bu nedenle üçüncü taraf IP kullanımı yalnızca işlevsel entegrasyon değil, güvenilirlik doğrulaması ve sahiplik koruması da gerektirmektedir (Bhunia ve ark., 2022; Hu ve ark., 2020).

Üretim, test ve saha kullanımı aşamalarında ise güvenliğin fiziksel yönü öne çıkabilmektedir. Dış kaynaklı dökümhaneler ve test merkezleri, netlist ya da fiziksel gerçekleştirme bilgisine erişebildikleri için fazla üretim, klonlama, sahtecilik ve donanım truva atı yerleştirme gibi tehditlere zemin hazırlayabilmektedir. Ürün saha kullanımına geçtiğinde ise fiziksel erişim, kurcalama, hata enjeksiyonu ve yan kanal analizi gibi saldırılar daha görünür hale gelebilmektedir. Başka bir ifadeyle, yaşam döngüsünün erken aşamalarında tasarım bilgisinin açığa çıkması öne çıkarken, geç aşamalarda fiziksel erişim temelli saldırılar ağır basmaktadır.

Bu yapı, tek katmanlı koruma yaklaşımlarının çoğu durumda yetersiz kalacağını göstermektedir. Örneğin yapısal gizleme sentez aşamasında yararlı olabilir. Ancak fazla üretim veya açık pazardaki sahtecilik sorununu tek başına çözemez. Benzer biçimde filigranlama sahiplik ispatı için etkili olsa da donanım truva atı yerleştirilmesini doğrudan önlemez. Bu nedenle koruma yöntemlerinin, yaşam döngüsünün ilgili aşaması ve tehdit türü dikkate alınarak seçilmesi gerekmektedir.

Tehdit modeli de yalnızca saldırganın kim olduğunu tanımlamakla sınırlı olmamalıdır. Saldırganın yaşam döngüsünün hangi aşamasında yer aldığı, hangi bilgiye erişebildiği ve hangi hedefle hareket ettiği de açık biçimde belirtilmelidir. Donanım güvenliği çalışmalarında yaygın yaklaşım, tasarım akışı içindeki güvenilir ve güvenilmez aktörleri ayırt etmektir. Bu çerçevede fikri mülkiyet sağlayıcısı açısından sistem bütünleştiricisi bir tehdit oluşturabilirken, sistem bütünleştiricisi açısından üçüncü taraf IP satıcısı veya dökümhane güvenilmez kabul edilebilir. Açık pazar aktörleri ve son kullanıcılar da fiziksel erişim yoluyla ek risk oluşturabilir (Anshul ve Sengupta, 2024; Bhunia ve ark., 2022).

Bu nedenle FPGA ve diğer donanım tabanlı sistemlerde geliştirilen fikri mülkiyet koruma yöntemleri değerlendirilirken,

yöntemin yaşam döngüsünün hangi aşamasını hedeflediği açık biçimde belirtilmelidir. Aksi durumda teorik olarak güçlü görünen bir çözüm, pratikte yanlış tehdit sınıfına uygulanmış olabilir. Yaşam döngüsü odaklı bu yaklaşım, sonraki başlıklarda ele alınacak tehditler ve koruma yöntemleri arasındaki ilişkiyi kurmak için temel bir çerçeve sunmaktadır.

4. FPGA VE DONANIM TABANLI SİSTEMLERDE BAŞLICA TEHDİTLER

FPGA ve diğer donanım tabanlı sistemlerde fikri mülkiyet korumasını zorlaştıran tehditler, yalnızca tasarım bilgisinin ele geçirilmesiyle sınırlı değildir. Tasarımın yapısal olarak çözümlenmesi, işlevsel olarak kopyalanması, fiziksel olarak çoğaltılması, kötü niyetli mantık eklenmesi veya çalışma sırasında bilgi sızdırılması gibi farklı saldırı türleri söz konusudur. Donanım güvenliği literatüründe bu tehditler çoğunlukla tersine mühendislik, klonlama ve sahtecilik, donanım truva atları, yetkisiz yeniden yapılandırma, yan kanal saldırıları ve hata enjeksiyonu başlıkları altında toplanmaktadır (Hu ve ark., 2020). FPGA sistemlerde bit akışı ve konfigürasyon altyapısı bu tehditleri daha görünür hale getirmektedir.

Tersine mühendislik, donanım fikri mülkiyetine yönelik en temel tehditlerden biridir. Amaç, tasarımın işlevsel veya yapısal bilgisini ortaya çıkarmaktır. Saldırgan, kayıt aktarım düzeyi, netlist, yerleşim verisi veya fiziksel örnek üzerinden devrenin nasıl çalıştığını anlamaya çalışır. FPGA sistemlerde bu süreç çoğu zaman bit akışının çözümlemesi ve konfigürasyon belleğinin incelenmesi üzerinden ilerlemektedir. Tersine mühendislik çoğu durumda diğer saldırıların ön adımıdır. Çünkü klonlama, kötü niyetli değişiklik ve tasarım sırrı çıkarma girişimleri genellikle önce sistemin anlaşılmasını gerektirmektedir (Bhunia ve ark., 2022; Açar ve ark., 2025).

Klonlama, sahtecilik ve fazla üretim doğrudan ekonomik kayıp doğuran tehditlerdir. Klonlama, özgün tasarımın lisanssız biçimde çoğaltılmasıdır. Sahtecilik, orijinal ürünü taklit eden fakat güvenilirliği belirsiz bileşenlerin pazara sürülmesini ifade etmektedir. Fazla üretim ise özellikle üretim aşamasında, lisanslanan miktarın üzerinde ürün üretilmesidir. Bu tehditler yalnızca gelir kaybına neden olmaz. Aynı zamanda düşük kaliteli veya kötü niyetli ürünlerin özgün üreticiye atfedilmesi nedeniyle itibar ve güvenilirlik sorunları da oluşturabilmektedir (Guin ve ark., 2014; Anshul ve Sengupta, 2024).

Donanım truva atları, tasarım içine kasıtlı olarak eklenen ve belirli koşullarda etkinleşen kötü niyetli mantık yapılarıdır. Bu tehdit özellikle üçüncü taraf IP kullanımı, güvenilmeyen tasarım araçları ve dış kaynaklı üretim süreçlerinde önem kazanmaktadır. Bir truva atı bilgi sızdırabilir, işlev bozabilir, performansı düşürebilir veya başka bir saldırıya zemin hazırlayabilir. En zorlayıcı yönü, çoğu zaman standart test koşullarında etkinleşmemesi ve bu nedenle fark edilmesinin güç olmasıdır (Akter ve ark., 2023; El Balbali ve Abou El Kalam, 2026).

Yetkisiz yeniden yapılandırma ve kurcalama, FPGA sistemlerde özel önem taşıyan başka bir tehdit grubudur. Bit akışının ele geçirilmesi, değiştirilmesi veya yeniden yüklenmesi, tasarımın hem işlevsel bütünlüğünü hem de fikri mülkiyet niteliğini riske atabilmektedir. Hata ayıklama bağlantı noktaları, Ortak Test Eylem Grubu (Joint Test Action Group, JTAG) arayüzleri ve kısmi yeniden yapılandırma mekanizmaları yeterince korunmadığında saldırgan için giriş noktası haline gelebilmektedir. Bu saldırılar yalnızca tasarım sırrını açığa çıkarmakla kalmaz, değiştirilmiş türev tasarımların oluşturulmasına da yol açabilmektedir (Açar ve ark., 2025).

Yan kanal saldırıları, sistemin mantıksal tanımından çok fiziksel davranışını hedef almaktadır.

Tablo 1. Donanım tabanlı sistemlerde fikri mülkiyet korumasını tehdit eden başlıca saldırı türleri ve karşılık gelen savunma yaklaşımları

Tehdit	Temel etki	Yaygın savunma sınıfı
Tersine mühendislik	Tasarım bilgisinin ve işlevsel yapının açığa çıkması	Gizleme, mantıksal kilitleme, kamuflajlama, redaksiyon
Klonlama / sahtecilik	Lisanssız çoğaltma, itibar kaybı, gelir kaybı	Filigranlama, parmak izleme, sayısal imza, üretim denetimi
Fazla üretim	Lisans sınırı dışında ürün çoğaltılması	Üretim sayacı, sahiplik kanıtı, üretim odaklı kontrol mekanizmaları
Donanım truva atı	Bilgi sızdırma, işlev bozma, arka kapı	Güvenilir IP doğrulaması, çalışma zamanı izleme, çok katmanlı savunma
Yetkisiz yeniden yapılandırma	Tasarımın değiştirilmesi veya türevlenmesi	Bitstream koruması, güvenli başlatma, kimlik doğrulama, anahtar yönetimi
Yan kanal saldırıları	Gizli veri veya anahtar sızıntısı	Maskeleme, gizleme, yan kanal dirençli tasarım, yapay zeka tabanlı tespit
Hata enjeksiyonu	Hatalı işlem, anahtar çıkarma, kimlik doğrulama atlatma	Hata tespiti, sensör tabanlı izleme, hataya dayanıklı mimari

Güç tüketimi, elektromanyetik yayılım, zamanlama farkları ve termal izler üzerinden elde edilen veriler, işlenen bilgi veya gizli anahtarlar hakkında çıkarım yapılmasını sağlayabilmektedir. Özellikle kriptografik modüller bu saldırılar için öncelikli hedef olabilmektedir. Son yıllarda yapay zeka ve derin öğrenme tabanlı analiz yöntemleri, bu saldırıları daha güçlü ve daha otomatik hale getirmiştir (El Balbali ve Abou El Kalam, 2026). Hata enjeksiyonu ise voltaj bozma, saat darbesi bozma, lazer enjeksiyonu veya elektromanyetik etki yoluyla sistemin belirli anlarda hatalı davranmaya zorlanmasına dayanmaktadır. Bu yaklaşım, kimlik doğrulama atlatma, kontrol akışını bozma veya anahtar çıkarma gibi sonuçlar doğurabilmektedir ve çoğu zaman yan kanal analizi ile birlikte kullanılmaktadır (Akter ve

ark., 2023). Bu tehditlerin temel etkileri ve bunlara karşı öne çıkan savunma sınıfları Tablo 1'de özetlenmiştir.

5. FİKRİ MÜLKİYET KORUMA YÖNTEMLERİ

FPGA ve donanım tabanlı sistemlerde fikri mülkiyet koruma yöntemleri genel olarak iki temel işleve sahiptir: tasarımın aidiyetini ve özgünlüğünü ispatlamak ya da tasarımın yetkisiz analizini, kopyalanmasını ve yeniden üretilmesini zorlaştırmak. İlk gruptaki yöntemler çoğunlukla sahiplik kanıtı üretirken, ikinci gruptaki yöntemler saldırının maliyetini artırmayı veya doğru işlevin elde edilmesini engellemeyi amaçlamaktadır. Bu ayrım, hangi koruma yaklaşımının hangi tehdit sınıfına karşı daha etkili olduğunu anlamak açısından önemlidir (Anshul ve Sengupta, 2024; Bhunia ve ark., 2022).

Aidiyet doğrulama odaklı yöntemlerin başında filigranlama gelmektedir. Bu yaklaşımda tasarımın yapısına veya sentez kararlarına geliştiriciye özgü gizli kısıtlar yerleştirilerek görünmez bir sahiplik izi oluşturulmaktadır. Özellikle yüksek seviyeli sentez tabanlı çalışmalarda zamanlama, kaynak ataması, bağlama ve kayıt ataması gibi aşamalara gömülen filigranların sahiplik ispatı açısından etkili olduğu gösterilmiştir (Koushanfar ve ark., 2005; Sengupta ve Roy, 2018; Rathor ve ark., 2023). Parmak izleme benzer bir mantığa dayanmaktadır. Ancak burada her lisanslı kopyaya özgü farklı bir tanımlayıcı üretilmektedir. Sayısal imza ve steganografi temelli yaklaşımlar ise tasarım kökenini doğrulamak veya görünür olmayan güvenlik izleri oluşturmak için kullanılmaktadır (Rathor ve Sengupta, 2020; Anshul ve Sengupta, 2024). Bu tür yöntemlerin en önemli avantajı, genellikle düşük maliyetle uygulanabilmeleridir. Buna karşılık temel sınırlılıkları, saldırıyı doğrudan önlememeleri ve daha çok saldırı sonrasında kanıt üretebilmeleridir.

Önleyici yöntemler ise tasarımın yapısal veya işlevsel çözümlemesini zorlaştırmayı amaçlamaktadır. Bu grupta en yaygın yaklaşımlar gizleme, mantıksal kilitleme, kayıt aktarım düzeyi kilitleme ve kamuflajlamadır. Yapısal gizleme, tasarımın işlevini korurken iç örgüsünü daha karmaşık hâle getirerek tersine mühendislik maliyetini artırmaktadır (Lao ve Parhi, 2015; Anshul ve Sengupta, 2024). Mantıksal kilitleme ise doğru işlevin yalnızca doğru anahtar uygulandığında elde edilmesini sağlamaktadır. Bu yöntem, lisanssız kullanım ve üretim zinciri kaynaklı tehditlere karşı güçlü bir yaklaşım olmakla birlikte, mantıksal doyurulabilirlik (SAT) tabanlı, yapısal ve makine öğrenmesi destekli saldırılar karşısında sürekli güçlendirilmek zorundadır (Yasin ve ark., 2016; Pilato ve ark., 2021; Gandhi ve ark., 2024). Kayıt aktarım düzeyi kilitleme, korumayı tasarım akışının daha erken aşamalarına taşıması bakımından önemlidir. Kamuflajlama, fiziksel inceleme yoluyla devre yapısının anlaşılmasını zorlaştırmayı amaçlamaktadır. Donanım redaksiyonu ve gömülü programlanabilir mantık alanı temelli çözümler ise kritik mantığı görünür tasarım alanından uzaklaştırarak benzer bir koruma sağlamaktadır (Bhunia ve ark., 2022). Ancak bu önleyici çözümler, çoğu durumda daha yüksek alan, güç ve tasarım karmaşıklığı maliyeti oluşturabilmektedir.

Koruma yöntemleri arasında seçim yapılırken yalnızca teorik güvenlik düzeyi değil, uygulanabilirlik, tasarım maliyeti, performans etkisi ve hedef platform da birlikte değerlendirilmelidir. Genel olarak tespit odaklı yöntemler daha düşük maliyetli ve daha kolay bütünleştirilebilir yapılarken, doğrudan önleme kabiliyetleri sınırlı olabilmektedir. Buna karşılık mantıksal kilitleme, gizleme ve kamuflajlama gibi yöntemler daha güçlü caydırıcılık sağlamaktadır. Ancak alan, güç ve gecikme üzerinde daha belirgin etki oluşturabilmektedir. FPGA sistemler açısından bakıldığında filigranlama, mantıksal kilitleme ve kayıt aktarım düzeyi kilitleme daha uygulanabilir

görünürken, kamuflajlama daha çok uygulamaya özel tümdevre tasarımlarında öne çıkmaktadır.

Bu değerlendirme, tek bir yöntemin tüm tehditlere karşı yeterli olmadığını göstermektedir. Uygulamada en etkili çözüm çoğu zaman, tehdit türüne göre seçilmiş çok katmanlı koruma birleşimleridir. Örneğin bit akışı koruması ile mantıksal kilitlemenin birlikte kullanılması, hem konfigürasyon düzeyinde hem işlevsel düzeyde güvenlik sağlayabilmektedir. Benzer biçimde filigranlama ile gizleme yöntemlerinin birlikte uygulanması, hem sahiplik ispatını hem de tersine mühendislik direncini artırabilmektedir (Bhunia ve ark., 2022; Gandhi ve ark., 2024).

6. FPGA ÖZELİNDE GÜVENLİK VE FİKRİ MÜLKİYET KORUMA MEKANİZMALARI

ASIC'ten farklı olarak FPGA sistemlerde tasarımın işlevsel karşılığı büyük ölçüde bit akışı içinde taşınır. Bu nedenle fikri mülkiyet koruması yalnızca kayıt aktarım düzeyi veya netlist ile sınırlı değildir. Yapılandırma verisinin korunması da aynı derecede önemli olmaktadır. (Açar ve ark., 2025; Pilato, 2022).

FPGA güvenliğinin temelinde bit akışı koruması yer almaktadır. Bit akışının ele geçirilmesi veya çözülmesi, tasarımın işlevsel yapısı hakkında doğrudan ya da dolaylı bilgi sağlayabilmektedir. Bu nedenle modern FPGA platformlarında bitstream şifreleme ve bitstream doğrulama temel savunma mekanizmalarıdır. Ancak bu koruma, yalnızca şifrelemeye değil, anahtarın güvenli saklanmasına ve yapılandırma sürecinin denetlenmesine de bağlı olmaktadır.

Güvenli başlatma, FPGA'in yalnızca doğrulanmış ve yetkili yapılandırmaları yüklemesini amaçlamaktadır. Özellikle saha güncellemesi alan veya uzaktan yönetilen sistemlerde bu

mekanizma, değiştirilmiş yapılandırmaların yüklenmesini önleyerek hem fikri mülkiyetin yetkisiz kullanımını hem de kötü niyetli işlev eklenmesini zorlaştırmaktadır. Anahtar yönetimi de bu yapının en kritik unsurudur. Anahtarların güvenli biçimde üretilmesi, saklanması ve kullanılması sağlanmadığında, diğer koruma katmanlarının etkisi önemli ölçüde azalabilmektedir.

Tablo 2. FPGA özelinde başlıca güvenlik ve fikri mülkiyet koruma mekanizmaları

Mekanizma	Koruduğu varlık	Temel amaç	Başlıca sınırlılık
Bitstream şifreleme	Konfigürasyon verisi	Bitstream'in okunmasını ve çözülmesini zorlaştırmak	Anahtar sızıntısına duyarlıdır
Bitstream doğrulama	Yapılandırma bütünlüğü	Değiştirilmiş bitstream yüklenmesini önlemek	Güvenilir kök doğrulama gerektirir
Güvenli başlatma	Başlangıç imajı ve yükleme zinciri	Yetkisiz yapılandırmaları engellemek	Yanlış yapılandırma açık oluşturabilir
Anahtar yönetimi	Kriptografik sırlar	Şifreleme ve doğrulamayı güvenceye almak	En kritik zafiyet noktalarındandır
JTAG / hata ayıklama kısıtlaması	İç sinyaller ve cihaz durumu	Yetkisiz analiz ve kurcalamayı önlemek	Geliştirme kolaylığı ile çelişebilir
Kısmi yeniden yapılandırma denetimi	Dinamik modüller	Yetkisiz modül yüklenmesini önlemek	Yönetimi karmaşık olabilir
Mantıksal kilitleme / tasarım içi koruma	İşlevsel tasarım yapısı	Yetkisiz kullanım ve analizi zorlaştırmak	Ek alan, güç ve gecikme maliyeti oluşturabilir

JTAG ve diğer hata ayıklama arayüzleri de önemli bir saldırı yüzeyi oluşturmaktadır. Bu arayüzler geliştirme ve test için gerekli olsa da, sınırlandırılmadıklarında cihaz durumu izleme, iç sinyalleri gözlemleme veya yapılandırma bilgisi çıkarma amacıyla kötüye kullanılabilmektedir. Bu nedenle üretim

sonrasında test ve hata ayıklama altyapısının sınırlandırılması FPGA güvenliğinin temel gereklilikleri arasındadır (Açar ve ark., 2025).

Üretici tarafından sağlanan cihaz içi güvenlik özellikleri önemli olmakla birlikte, tek başına yeterli değildir. Bitstream şifreleme ve güvenli başlatma cihaz düzeyinde koruma sağlarken, tasarımın işlevsel yapısını korumak için mantıksal kilitleme veya tasarım içi gizleme gibi ek yöntemlere ihtiyaç duyulabilmektedir. Bu nedenle FPGA güvenliği, cihaz düzeyi ve tasarım düzeyi savunmaların birlikte kullanıldığı çok katmanlı bir yapı olarak ele alınmalıdır. Bu mekanizmalar Tablo 2'de özetlenmiştir.

Tablo 2'nin gösterdiği gibi FPGA güvenliği tek bir mekanizmaya dayanmamaktadır. Bitstream şifreleme ve güvenli başlatma yapılandırma zincirini korurken, tasarım içi koruma teknikleri işlevsel fikri mülkiyetin açığa çıkmasını zorlaştırabilmektedir.

7. GÜVENLİK, PERFORMANS VE MALİYET DENGESİ

Donanım tabanlı sistemlerde kullanılan her fikri mülkiyet koruma yöntemi belirli bir maliyet üretmektedir. Bu maliyet çoğunlukla alan kullanımı, güç tüketimi, gecikme ve tasarım karmaşıklığı olarak ortaya çıkmaktadır. Bu nedenle koruma yöntemleri değerlendirilirken yalnızca saldırı dayanımı değil, sistem verimliliği üzerindeki etkileri de dikkate alınmalıdır. Özellikle kaynakları sınırlı FPGA platformlarında ve gerçek zamanlı uygulamalarda, güçlü koruma sağlayan fakat yüksek alan ya da zamanlama cezası getiren çözümler pratikte uygun olmayabilir (Anshul ve Sengupta, 2024; Gandhi ve ark., 2024).

Alan maliyeti, güvenlik mekanizmalarının en doğrudan etkilerinden biridir. Filigranlama ve bazı sayısal imza temelli

yöntemler daha sınırlı ek kaynak gerektirirken, mantıksal kilitleme, kamuflajlama ve redaksiyon gibi yöntemler daha yüksek donanım yükü oluşturabilir. FPGA sistemlerde bu durum, bakış tablosu, tetikleyici, blok bellek ve yönlendirme kaynaklarının tüketimi üzerinden hissedilebilir.

Güç tüketimi ve gecikme de önemli ödünleşim alanlarıdır. Ek güvenlik mantığı, daha uzun veri yolları ve sürekli çalışan denetim yapıları dinamik ve statik güç tüketimini artırabilir. Benzer biçimde güvenlik amacıyla eklenen mantık, kritik yol üzerinde yer aldığında gecikme artışı oluşabilir ve maksimum saat frekansı düşebilir. Tasarım karmaşıklığı ise sentez, doğrulama, hata ayıklama ve bakım süreçlerini zorlaştırabilmektedir.

Bu nedenle en uygun yaklaşım, her durumda en güçlü korumayı seçmek değildir. Tehdit modeli ile sistemin kaynak ve performans sınırlarını dengeli biçimde eşleştirmektir. FPGA tabanlı sistemlerde etkili fikri mülkiyet koruması, güvenlik ile verimlilik arasında bilinçli biçimde kurulan bu dengeye bağlıdır.

8. SONUÇ

FPGA ve donanım tabanlı sistemlerde fikri mülkiyet koruması, günümüz yarı iletken ekosisteminin temel güvenlik konularından biridir. Donanım IP'lerinin yüksek ekonomik değeri, yeniden kullanılabilir yapıları ve çok aktörlü tasarım-üretim zinciri, bu varlıkları tersine mühendislik, klonlama, sahtecilik, fazla üretim, donanım Truva atı, yan kanal saldırıları ve yetkisiz yeniden yapılandırma gibi tehditlere açık hale getirmektedir.

Bu bölümde ele alınan çalışmalar, tek bir koruma yönteminin tüm tehditlere karşı yeterli olmadığını göstermektedir. Filigranlama, parmak izleme, sayısal imza ve

steganografi gibi yöntemler sahiplik ispatı ve korsan kullanımın tespiti açısından değerli araçlar sunarken; gizleme, mantıksal kilitleme, kayıt aktarım düzeyi kilitleme, kamuflajlama ve FPGA'ye özgü bitstream güvenliği mekanizmaları daha aktif koruma sağlamaktadır. Ancak her yöntemin etkili olduğu tehdit sınıfı farklıdır.

Bu nedenle etkili fikri mülkiyet koruması, yaşam döngüsü boyunca tehdit odaklı ve çok katmanlı bir yaklaşımla kurulmalıdır. Özellikle FPGA sistemlerde bitstream koruması, güvenli başlatma, anahtar yönetimi ve tasarım içi koruma tekniklerinin birlikte değerlendirilmesi gerekmektedir. Sonuç olarak bu alandaki başarı, uygun koruma yöntemlerinin tehdit modeline göre seçilmesine ve güvenlik, performans ile maliyet arasında dengeli bir mimari kurulmasına bağlıdır.

KAYNAKÇA

Açar, T., Tiryakioğlu, F., & Örs Yalçın, S. B. (2025). Logic locking-based FPGA system design for third-party IP protection. *2025 33rd Signal Processing and Communications Applications Conference (SIU)*, 1–4.

Akter, S., Khalil, K., & Bayoumi, M. (2023). A survey on hardware security: Current trends and challenges. *IEEE Access*.

Anshul, A., & Sengupta, A. (2024). A survey of high-level synthesis based hardware security approaches for reusable IP cores. *IEEE Circuits and Systems Magazine*.

Bhunia, S., Das, A., Fazzari, S., Kammler, V., Kehlet, D., Rajendran, J., & Srivastava, A. (2022). Hardware IP protection against confidentiality attacks and evolving role of CAD tool. In *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*.

El Balbali, H., & Abou El Kalam, A. (2026). Security threats and AI-based detection techniques in IoT chips. *Chips, 5*(1), 9.

Gandhi, J., Shekhawat, D., Santosh, M., & Pandey, J. G. (2024). Emerging frontiers and limitations of logic locking for secure IC design. In *2024 IEEE 17th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC)*.

Guin, U., DiMase, D., & Tehranipoor, M. (2014). Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. *Proceedings of the IEEE, 102*(8), 1207–1228.

Hu, W., Chang, C.-H., Sengupta, A., Bhunia, S., Kastner, R., & Li, H. (2020). An overview of hardware security and trust:

Threats, countermeasures, and design tools. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*.

Koushanfar, F., Hong, I., & Potkonjak, M. (2005). Behavioral synthesis techniques for intellectual property protection. *ACM Transactions on Design Automation of Electronic Systems, 10*(3), 523–545.

Lao, Y., & Parhi, K. K. (2015). Obfuscating DSP circuits via high-level transformations. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 23*(5), 819–830.

Pilato, C. (2022). High-level methods for hardware IP protections: Solutions, trends, and challenges. *IEEE Design & Test*.

Pilato, C., Chowdhury, A. B., Sciuto, D., Garg, S., & Karri, R. (2021). ASSURE: RTL locking against an untrusted foundry. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 29*(7), 1306–1318.

Rajendran, J. V. (2017). An overview of hardware intellectual property protection. In *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*.

Rathor, M., & Sengupta, A. (2020). IP core steganography using switch-based key-driven hash-chaining and encoding for securing DSP kernels used in consumer electronics systems. *IEEE Transactions on Consumer Electronics, 66*(3), 251–260.

Rathor, M., Anshul, A., Bharath, K., Chaurasia, R., & Sengupta, A. (2023). Quadruple phase watermarking during high level synthesis for securing reusable hardware intellectual property cores. *Computers and Electrical Engineering, 105*, 108476.

Sengupta, A., & Roy, D. (2018). Triple-phase watermarking for reusable IP core protection during architecture synthesis. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 37*(4), 742–755.

Shamsi, K., Li, M., Plaks, K., Fazzari, S., Pan, D. Z., & Jin, Y. (2019). IP protection and supply chain security through logic obfuscation: A systematic overview. *ACM Transactions on Design Automation of Electronic Systems, 24*(6), 1–36.

Yasin, M., Rajendran, J. J. V., Sinanoglu, O., & Karri, R. (2016). On improving the security of logic locking. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 35*(9), 1411–1424.

ELECTRYPTION: BLOK ZİNCİR TABANLI E-OYLAMA SİSTEMİ

Meryem SOYSALDI ŞAHİN[1]

İbrahim GÜNEŞ[2]

İshak DURAN[3]

Cuma TALJİBİNİ[4]

1. GİRİŞ

Demokratik sistemlerin yaygınlaşması ve yönetim süreçlerinin halk iradesine dayandırılması ile birlikte, seçim kavramı toplumsal ve politik açıdan merkezi bir öneme sahip olmuştur. Seçim süreçleri, aday belirleme aşamasından oyların sayılmasına kadar uzanan, büyük ölçüde insan müdahalesine dayalı karmaşık süreçlerden oluşmaktadır. Bu süreçler, zaman içinde geleneksel ve oturmuş yöntemlerle yürütülse de, doğal olarak hataya ve manipülasyona açıktır. Özellikle merkezi otoriteye bağımlılık, şeffaflık eksikliği ve dolandırıcılık riskleri, demokratik süreçlerin güvenilirliğini olumsuz yönde etkileyebilmektedir.

Geleneksel oylama sistemleri; şeffaflık eksikliği, yüksek maliyetler, lojistik zorluklar ve sahteciliğe ya da manipülasyona

[1] Dr. Öğr. Üyesi, Ondokuz Mayıs Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, ORCID: 0000-0002-1674-2768

[2] Bilgisayar Mühendisi, Ondokuz Mayıs Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, ORCID: 0009-0003-1168-3812.

[3] Bilgisayar Mühendisi, Ondokuz Mayıs Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, ORCID: 0009-0001-6384-269X.

[4] Bilgisayar Mühendisi, Ondokuz Mayıs Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, ORCID: 0009-0005-8544-7235.

açık olma gibi sorunlarla uzun süredir karşı karşıyadır. Elektronik oylama sistemleri bu sorunların bir kısmını azaltmak için geliştirilmiş olsa da, merkeziyetçi yapıları sebebiyle güven, güvenilirlik ve veri bütünlüğü konusunda yeni endişeler doğurmuştur. Oysaki demokratik toplumların temel gerekliliklerinden biri, her bir oyun doğru bir şekilde kaydedildiğinden, sayıldığından ve değiştirilmeden korunduğundan emin olunmasıdır. Bu noktada, güvenli, şeffaf ve maliyet etkin oylama mekanizmalarına duyulan artan ihtiyaç, blok zinciri gibi yeni nesil teknolojilerin seçim süreçlerinde kullanılmasına yönelik motivasyonu artırmaktadır. Blok zincirinin değiştirilemezlik, merkeziyetsizlik ve doğrulanabilirlik gibi temel özellikleri, güvenilir elektronik oylama platformları geliştirmek için güçlü bir zemin sunmaktadır. Akıllı sözleşmeler ve modern kriptografik yöntemler kullanılarak seçmen kimlik doğrulaması yapılabilmekte, oy gizliliği korunabilmekte ve seçim sonuçları tüm paydaşlar tarafından denetlenebilir hâle gelmektedir.

Bu çalışmanın motivasyonu, hem geleneksel hem de merkeziyetçi elektronik oylama sistemlerinin eksikliklerini giderecek bir çözüm geliştirme ihtiyacından doğmaktadır. Önerilen blok zinciri tabanlı elektronik oylama sistemi; seçim süreçlerine duyulan güveni artırmayı, erişilebilirliği sayesinde seçmen katılımını yükseltmeyi ve seçimlerin operasyonel maliyetlerini azaltmayı amaçlamaktadır. Bu çalışmanın nihai hedefi, üniversite ölçeğinden ulusal seçimlere kadar farklı bağlamlarda uygulanabilecek ölçeklenebilir, şeffaf ve güvenli bir seçim modeli sunarak demokratik süreçlerin gelişimine katkıda bulunmaktır. Bu doğrultuda önerilen sistemin başlıca bilimsel katkıları aşağıda sıralanmaktadır:

- Önerilen sistem, seçmenin kripto hesabı veya özel anahtar yönetimiyle doğrudan uğraşmasını gerektirmeyen bir mimari sunarak blok zinciri tabanlı

oylama sistemlerinde yaygın olarak karşılaşılan kullanılabilirlik sorunlarını azaltmaktadır.

- Modelde adaylar, pasif blok zinciri adresleri yerine bağımsız akıllı sözleşmeler olarak modellenerek oyların sözleşme mantığı çerçevesinde yönetilmesi ve aday bazlı şeffaf, değiştirilemez veri takibinin sağlanması mümkün kılınmaktadır.
- Oy verme süreci, seçmenin sahip olduğu admin tokenlarını ilgili aday akıllı sözleşmesine yetkilendirme ve transfer etmesi prensibine dayandırılarak oyların kriptografik olarak doğrulanabilir, izlenebilir ve bütünlüğü korunmuş biçimde kaydedilmesi sağlanmaktadır.
- Seçim sürecinin tamamı zincir üzerinde yürütülerek oy verme işlemleri ve seçim sonrası kayıtlar Ethereum blok zinciri üzerinde saklanmakta; ayrıca aday akıllı sözleşmeleri ile bu sözleşmelerin adres listesini tutan ana akıllı sözleşme de zincir üzerinde muhafaza edilerek geriye dönük denetlenebilirlik ve değiştirilemezlik garanti altına alınmaktadır.
- Önerilen mimari, farklı ölçeklerdeki seçim senaryolarına uyarlanabilecek biçimde tasarlanarak hem küçük ölçekli kurumsal seçimlerde hem de daha geniş kapsamlı organizasyonlarda uygulanabilir bir model sunmaktadır.

1.1. Organizasyon

Bu çalışmanın ilerleyen bölümleri şu şekilde organize edilmiştir: Bölüm 2'de, elektronik oylama ve blok zinciri teknolojisi alanındaki mevcut sistemler incelenmiş, kullanılan yöntemler ve karşılaşılan eksiklikler değerlendirilmiştir. Bölüm 3'te, blok zincir teknoloji ve çalışma yapısı ele alınmıştır. Bölüm

4'te, önerilen sistemin Ethereum platformu üzerindeki tasarımı, kullanılan akıllı sözleşmeler ve seçim sürecinin teknik aşamaları detaylandırılmıştır. Son bölümde ise sonuçlara yer verilmiştir.

2. LİTERATÜR ÖZETİ

Bu bölümde blok zincir teknolojisi kullanılarak geliştirilen elektronik oylama sistemleri incelenmiştir. Literatürde önemli bir araştırma yönü, Ethereum tabanlı akıllı sözleşmeler aracılığıyla oy verme sürecinin otomatikleştirilmesine odaklanmaktadır. Naik, Mishra, Prajapati ve Pandey (2023), Swar, Nimkar, Shinde, Lotlikar ve Reddy (2023), Abdulah ve Adnan (2023), Dagher, Marella, Milojkovic ve Mohler (2018), Singh, Singh, Verma ve Dwivedi (2023), Vairam, Sarathambekai ve Balaji (2021), Koç, Çabuk, Yavuz ve Dalkılıç (2024), Fusco, Lunesu, Pani ve Pinna (2024), Alvi, Uddin, Islam ve Ahamed (2024), Kumar E, Gadli, Parihar, Prasath, Gowtham, ve Kumar. (2024) ile Kumari, H., Veni, Purohit ve M. (2024) tarafından gerçekleştirilen çalışmalarda akıllı sözleşmeler kullanılarak oyların blok zinciri üzerine kaydedilmesi sağlanmıştır. Bu sistemlerde seçmenler kripto hesapları aracılığıyla sisteme kaydolmakta, oy verme işlemi bir blok zinciri işlemi olarak gerçekleştirilmekte ve her bir oy işlem kimliği (Transaction ID) üzerinden doğrulanabilmektedir. Böylece oyların değiştirilemezliği ve izlenebilirliği teknik olarak garanti altına alınmaktadır.

Literatürde ayrıca blok zinciri altyapısı kullanılarak geliştirilen çeşitli oylama platformları da bulunmaktadır. Paredes, Medina ve Moroco (2022) tarafından geliştirilen Boxting sistemi, blok zinciri tabanlı bir oylama platformu olarak tasarlanmış ve oyların güvenli ve değiştirilemez bir yapıda saklanması hedeflenmiştir. Benzer şekilde Birol, İskender, Özkul ve Topallı (2024) tarafından geliştirilen Votamat sistemi, blok zinciri tabanlı

bir seçim platformu önererek seçim süreçlerinde şeffaflık ve güvenliğin artırılmasını amaçlamıştır. Ayrıca Khoury, Kfoury, Kassem ve Harb (2024) tarafından önerilen merkeziyetsiz oylama platformunda Ethereum blok zinciri kullanılarak oyların doğrulanması ve güvenli biçimde saklanması sağlanmıştır.

Bazı çalışmalarda sistemlerin test ağları üzerinde çalıştırıldığı ve performans analizlerinin gerçekleştirildiği görülmektedir. Özellikle Dagher ve ark. (2018), Koç ve ark. (2024) ve Fusco ve ark. (2024) çalışmalarında Ropsten ve Rinkeby gibi Ethereum test ağları üzerinde uygulamalar geliştirilmiş ve işlem maliyetleri, gecikme süreleri ile sistem ölçeklenebilirliği değerlendirilmiştir. Bu çalışmaların temel amacı seçim süreçlerinde merkezi otoriteye duyulan güveni azaltarak merkeziyetsiz bir yapı oluşturmaktır.

Literatürde yer alan bir diğer yaklaşım ise oy hakkının blok zinciri üzerinde temsil edilen dijital bir varlık olarak modellenmesine dayanmaktadır. Bu kapsamda Wadhwa (2024) ile Vo-Cao-Thuy, Cao-Minh, Dang-Le-Bao ve Nguyen (2024) çalışmalarında NFT tabanlı oylama sistemleri önerilmiştir. Her iki modelde de akıllı sözleşmeler kullanılarak oy işlemlerinin doğrulanması sağlanmaktadır. Özellikle Vo-Cao-Thuy ve ark. (2024) tarafından geliştirilen Votereum sisteminde sonuç doğrulama mekanizmasının sistem tasarımına entegre edildiği görülmektedir. Hjálmarsson, Hreiðarsson, Hamdaqa ve Hjálmtýsson (2018) çalışmasında ise ERC-721 standardı kullanılarak her seçmene benzersiz bir NFT atanmış ve oy kullanma işlemi bu NFT'nin transferi şeklinde modellenmiştir. Benzer şekilde Pranitha, Sah, Rukmini, Kumar, Shankar ve Padhy, (2024) seçmenlere tek kullanımlık bir oy tokeni tahsis ederek mükerrer oy kullanımını yapısal olarak engellemeyi amaçlamıştır.

Bazı araştırmalar doğrudan uygulama katmanına değil, blok zinciri alt yapısının temelini oluşturan konsensüs ve doğrulama mekanizmalarına odaklanmaktadır. Tandon, Satiram, Singh, Porwal ve Maurya (2022), Abdulah ve Adnan (2023), Vairam ve ark. (2021) ve Yi (2019) çalışmalarında Proof of Work (PoW) temelli doğrulama mekanizmaları kullanılarak güvenli blok üretimi ve işlem doğrulama süreçleri incelenmiştir. Bunun yanı sıra Joni, Rahat, Tasnin, Ghose ve Gaur (2023) tarafından geliştirilen HAC-Bchain sisteminde hibrit bir konsensüs algoritması ile kategori tabanlı parçalama (sharding) mimarisi önerilmiş ve işlem yükünün dağıtılması hedeflenmiştir.

Literatürde seçmen doğrulama mekanizmalarının güçlendirilmesine yönelik çalışmalar da bulunmaktadır. Singh, Kaur, Agarwal ve Idrees (2024) Ethereum tabanlı bir sistemde mükerrer oy kullanımını önlemek amacıyla retina taraması ve devlet veri tabanlarının kullanılmasını önermiştir. Ancak bu yaklaşımın ölçeklenebilirlik ve gizlilik açısından çeşitli riskler taşıdığı belirtilmiştir. Balti, Prabhu, Shahi, Dahifale ve Maheta (2024) seçmen doğrulamasını tek kullanımlık parola (One Time Password – OTP) ile gerçekleştirmiştir. Benzer şekilde Joseph, Pandey Khari, Kumar ve Singh (2024) ile Othman, Muhammed, Muhammed, Mosleh ve Mujahid, (2024) çalışmalarında OTP, yüz tanıma ve biyometrik verilerin birlikte kullanıldığı çok katmanlı güvenlik mekanizmaları önerilmiştir. Ayrıca Indukuri, Ulvalapudi, Eguram, Gajula ve Nichena (2023) dijital kimlik ve biyometrik verilerden elde edilen hash değerleri kullanarak oy takibini gerçekleştirmiş ve doğrulama sürecini kriptografik özet değerler üzerinden yürütmüştür.

Öte yandan bazı çalışmalar doğrudan sistem performansı, ölçeklenebilirlik ve kriptografik güvenlik analizine odaklanmaktadır. Prasad (2024) bölge bazlı ölçeklenebilir bir blok zinciri mimarisi önererek işlem yükünün dağıtılmasını hedeflemiştir. Luo (2024) ise Schnorr algoritmasına dayalı vekil

çoklu imza teknolojisi kullanarak doğrulama hızının artırılabileceğini ve veri boyutunun azaltılabileceğini göstermiştir. Ayrıca Taş ve Tanrıöver (2020) tarafından yapılan sistematik literatür incelemesinde 63 farklı çalışma analiz edilmiş ve merkezi sistemlerdeki güvenlik açıkları değerlendirilmiştir. Bu çalışmada özellikle gizlilik ve ölçeklenebilirliğin blok zincir tabanlı oylama sistemlerinde çözülmesi gereken en önemli teknik zorluklar arasında yer aldığı vurgulanmıştır. Bunun yanında Lauer (2024) elektronik oylama sistemlerinin güvenlik ve seçim bütünlüğü açısından çeşitli riskler barındırabileceğini belirtmiş ve dijital seçim sistemlerinin dikkatli bir şekilde tasarlanması gerektiğini ifade etmiştir. Bu bölümde ele alınan çalışmaların karşılaştırmalı analizi Tablo 1'de sunulmaktadır.

Tablo 1. Literatürde kullanılan teknolojiler

Kaynak	Veri Tabanı	Truffle	Ganache	MetaMask	Dağıtık Defter	Konsensüs Algoritması	NFT	Akıllı Sözleşme	Geth
Abdulah ve Adnan, (2023)		✅	✅	✅	✅			✅	
Naik, Mishra, Prajapati ve Pandey, (2023)	✅				✅	✅		✅	
Indukuri, Ulvalapudi, Eguram, Gajula, ve Nichena, (2023)	✅	✅	✅	✅				✅	
Paredes, Medina, ve Moroco, (2022)	✅							✅	
Vairam, Sarathambekai, ve Balaji, (2021)		✅	✅	✅	✅	✅		✅	
Swar, Nimkar, Shinde, Lotlikar, ve Reddy, (2023)		✅	✅	✅				✅	
Singh, Singh, Verma, ve Dwivedi, (2023)	✅				✅			✅	
Tandon, Satiram, Singh, Porwal, ve Maurya, (2022)						✅			

Birol, İskender, Özkul ve Topallı, (2024)	✅								
Wadhwa, (2024)							✅	✅	
Fusco, Lunesu, Pani, ve Pinna, (2024)								✅	
Prasad, (2024)		✅				✅		✅	✅
Hjálmarsson, Hreiðarsson, Hamdaqa ve Hjálmtýsson, (2018)								✅	✅
Dagher, Marella, Milojkovic, ve Mohler, (2018)				✅				✅	
Khoury, Kfoury, Kassem, ve Harb, (2024)								✅	
Yi, (2019)					✅	✅			
Singh, Kaur, Agarwal, ve Idrees, (2024)								✅	
Taş ve Tanrıöver, (2020)						✅		✅	
Koç, Çabuk, Yavuz, ve Dalkılıç, (2024)								✅	
Vo-Cao-Thuy, Cao-Minh, Dang-Le-Bao, ve Nguyen, (2024)							✅	✅	
Kumar E, Gadli, Parihar, Prasath, Gowtham, ve Kumar, (2024)						✅		✅	
Kumari, H, Veni, Purohit, ve M, (2024)			✅	✅				✅	
Balti, Prabhu, Shahi, Dahifale, ve Maheta, (2024)					✅				
Alvi, Uddin, Islam, ve Ahamed, (2024)		✅	✅	✅				✅	
Luo, (2024)								✅	
Joseph, Pandey, Khari, Kumar ve Singh, (2024)								✅	
Pranitha, Sah, Rukmini, Kumar, Shankar, ve Padhy, (2024)						✅		✅	
Joni, Rahat, Tasnin, Ghose, ve Gaur, (2023)	✅					✅			
Othman, Muhammed, Muhammed, Mosleh, ve Mujahid, (2024)								✅	

3. BLOK ZİNCİRİ TEKNOLOJİSİ

Blok zinciri, merkezi olmayan bir veri tabanına benzemektedir. Ancak geleneksel veri tabanlarından farklı olarak, veriler bağlı listeler benzeri bir veri yapısı ile tutulmaktadır ve bu yapının her bir birimi blok olarak adlandırılmaktadır. Bloklar, birbirine kriptografik bir özetleme yöntemi olan hash algoritması ile bağlanmaktadır. Birbirine bağlı olan her bir blok gövde ve başlıktan oluşmaktadır. Gövde içerisinde işlem sayacı ve işlemler tutulmaktadır. Başlık içerisinde blok versiyonu, Merkle ağaç kökü özeti, zaman damgası, nBits, nonce değeri ve bir önceki bloğun hash değeri tutulmaktadır. Bir blok oluşturulduğunda, o bloğun hash değeri bir sonraki bloğun başlık bilgisine eklenmektedir. Bu şekilde bloklar, zincir şeklinde birbirine bağlanmaktadır.

Blok zincirini geleneksel veri tabanından ayıran özellikler bulunmaktadır. Merkeziyetsizlik ve dağıtık yapı sayesinde blok zinciri tek bir merkezde bulunmamakta, ağdaki tüm düğümlerde kopyalanmış şekilde yer almaktadır. Manipüle edilemezlik, blokların hash değeri ile birbirine bağlı olmasından kaynaklanmakta; en küçük değişiklik zincirin bütünlüğünü bozmakta ve sonraki tüm blokların hash değerlerinin değişmesine sebebiyet vermektedir. Manipülasyonun tespit edilebilirliği, ağdaki tüm düğümlerde zincirin tamamının kopyasının bulunmasından kaynaklanmakta; herhangi bir düğümde bulunan zincirdeki değişiklik diğer düğümlerdeki zincirler ile onu uyumsuz yapmakta ve bu sayede manipülasyon kolaylıkla anlaşılmaktadır. Dağıtık olması ve kriptografik yöntem ile zincir oluşması, onu güvenilir ve değiştirilemez yapmaktadır. Zincire blok ekleme işlemi, ağdaki tüm düğümler tarafından zaman damgalı algoritmalar aracılığıyla mutabakat kurallarına göre onayladığı blokların zincire eklenmesi şeklinde gerçekleşmektedir. Tamamen şeffaf ve güvenilir olmasından dolayı herkes zincirdeki verileri görebilmekte ve dijital imza ile

veri transferinde veriler doğrulanabilmektedir. Blok zincirinde bulunan ilk blok, önceki bloğu bulunmayan genesis bloğu olarak adlandırılmaktadır.

4. YÖNTEM

Bu bölümde önerilen sistem ayrıntılı olarak ele alınmaktadır. Öncelikle sistemin teknik altyapısı ve mimari bileşenleri açıklanmakta, ardından oy verme sürecine ilişkin işleyiş mekanizması sistematik biçimde ortaya konulmaktadır. Son olarak, kullanıcı ara yüzünün tasarım prensipleri ve operasyonel çalışma süreci detaylı olarak sunularak sistemin uygulama düzeyindeki işlevselliği değerlendirilmektedir.

4.1. Genel Sistem Tanımı

Önerilen sistem için Ethereum blok zinciri ağı tercih edilmiştir. Özel Ethereum ağını oluşturmak için Hardhat geliştirme aracı kullanılmıştır. Bu sayede özel Ethereum blok zinciri ağı oluşturulmuş olup ağ içerisinde belli işlevler gerçekleştirilecek ve işlem sonuçları zincire blok olarak kaydedilecektir. Şekil 1'de kullanılan teknolojiler ile seçim arasındaki ilişki somutlaştırılmıştır.

Şekil 1. İlişkili Teknolojiler

Ağ üzerinde seçmenin işlem yapabilmesi, özellikle oy kullanabilmesi için ağ içerisinde bir hesabı olması gerekmektedir. Ancak sistem, seçmenin oy kullanmak için kripto hesap oluşturma, blok zinciri kripto gibi teknik bilgi ve becerilere sahip olmasına gerek olmadığı fikrini savunmaktadır. Bu nedenle, sisteme kayıt olan seçmene arka uç tarafından hali hazırda var olan hesaplardan anonim bir şekilde tahsis edilmesiyle ya da kayıt esnasında yeni bir hesap oluşturularak seçmene kripto hesabı tahsis edilmektedir. Ethereum ağına dağıtılacak ve işlevler gerçekleştirecek olan akıllı sözleşmeler Solidity programlama dili ile yazılmıştır.

Önerilen sistem, geleneksel merkezi veritabanı yapısı ile blok zinciri teknolojisini hibrit bir yaklaşımla birleştirmektedir. Bu mimarinin amacı; salt merkezi sistemlerin şeffaflık ve denetlenebilirlik açığını, salt dağıtık sistemlerin ise kimlik yönetimi ve performans zorluklarını aynı anda ele alabilmektir. Bu hibrit yapı, kullanıcı kimlik doğrulama gibi yüksek frekanslı işlemleri merkezi MySQL veritabanında yönetirken; oy kayıtları gibi yüksek güvenlik, değiştirilemezlik ve şeffaflık gerektiren kritik verileri blok zinciri üzerinde gerçekleştirmektedir.

4.2. Sistem Mimarisi

4.2.1. Akıllı Sözleşmeler

Ethereum blok zinciri ağına dağıtılmış ya da işleyiş esnasında dağıtılacak olan akıllı sözleşmeler VoteToken, VotingRegister ve Aday akıllı sözleşmeleridir. Şekil 2'de belirtilen bu sözleşmeler şu şekilde açıklanabilir:

- VoteToken: Bu akıllı sözleşmenin temel amacı; seçim süresince kullanılacak tokenların üretimi, yetkilendirilmesini ve güvenli bir şekilde transfer edilmesini sağlamaktır. Bu amaçları ilgili seçimin biteceği zaman, seçmenin ilgili seçim için oy kullanıp kullanmadığı, seçmenin ilgili seçim için yetkilendirilip

yetkilendirilmediği, ilgili seçimde yetkilendirilme yapılıp yapılmadığı gibi parametrelerin kontrolü sayesinde yapmaktadır.

- Aday: Bu akıllı sözleşmenin temel amacı; seçime giren adayların bilgilerini tutmak, aday bilgilerini görüntülemek, seçmenlerin adaylara oy vermesini ve adayların anlık oy miktarını görüntülemeyi sağlamaktır.

Şekil 2. Akıllı Sözleşmeler

Her bir aday aslında bir akıllı sözleşmedir ve seçmenler, ilgili adayın akıllı sözleşmesine token göndererek oy kullanır.

- VotingRegister: Bu akıllı sözleşmenin temel amacı, seçim sonunda seçim isimleri ile o seçimin aday adreslerini eşleştirip saklamak ve bitmiş olan seçimlerdeki adayların aday akıllı sözleşme adreslerini görüntülemektir.

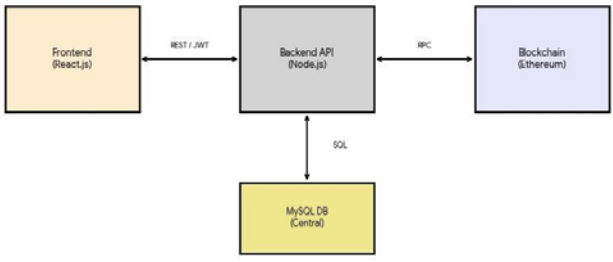
4.2.2. Arka Uç (Backend) Katmanı

Sistem, iki farklı kullanıcı tipini desteklemektedir: seçmenler ve sistem yöneticileri. Kullanıcı bilgileri MySQL veritabanında güvenli bir şekilde saklanmaktadır. Parola güvenliği, endüstri standardı olan bcrypt algoritması kullanılarak özetleme (hashing) ve tuzlama (salting) yoluyla sağlanmaktadır.

Kimlik doğrulama süreci, durum bilgisi tutmayan ve ölçeklenebilir bir yapı sağlayan JSON Web Token (JWT) standardına dayanmaktadır (token geçerlilik süresi: 24 saat). Seçmen kayıt işlemi sırasında, sistem T.C. kimlik numarasının benzersizliğini veritabanı düzeyinde kontrol etmekte ve her seçmene otomatik olarak bir blok zinciri cüzdan adresi atamaktadır. Bu yaklaşım, teknik bilgisi olmayan seçmenlerin cüzdan oluşturma ve özel anahtar yönetimi gibi karmaşık süreçlerini soyutlayarak kullanıcı deneyimini basitleştirmektedir. Bu atama işlemi, Hardhat geliştirme ortamı tarafından sağlanan mevcut Ethereum adreslerinden gerçekleştirilmektedir.

MySQL veritabanı, kaynak verimliliği ve performans sağlamak amacıyla bir bağlantı havuzu (connection pool) mimarisi (maksimum 10 eşzamanlı bağlantı) kullanılarak yönetilmektedir. Veritabanı şeması, secmenler ve admin tabloları ile temel veri yapılarını içermektedir.

REST mimarisi temel alınarak geliştirilmiş uç noktalar (endpoints), ön uç (frontend) ile blok zinciri katmanı arasında köprü görevi görmektedir. Sistem, CORS (Farklı Kökenler Arası Kaynak Paylaşımı) politikalarını destekleyerek farklı kökenlerden gelen isteklere kontrollü izin vermektedir. API güvenliği, yetkisiz erişimi engellemek amacıyla ara katman yazılımı (middleware) tabanlı JWT yetkilendirme mekanizmaları kullanılarak sağlanmaktadır. Şekil 3'te temel tasarım şeması gösterilmektedir.



Şekil 3. Temel Tasarım Şeması

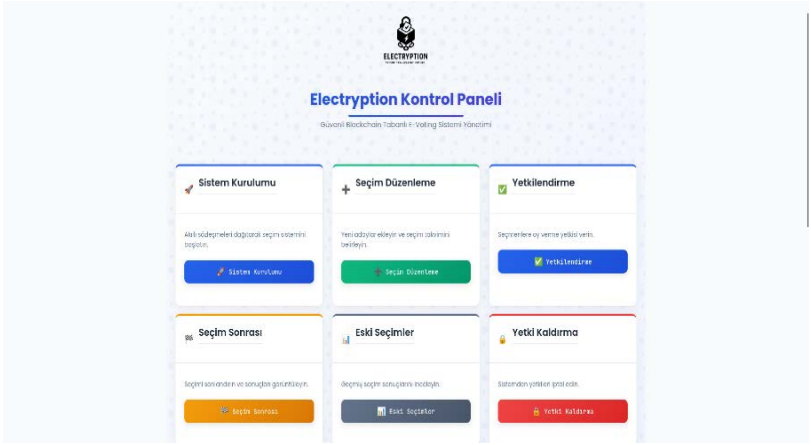
4.2.3 Ön Uç (Frontend) Katmanı

Ön uç katmanı, modüler, yeniden kullanılabilir bileşenler ve verimli durum yönetimi kabiliyetleri nedeniyle React.js (v18.x) kütüphanesi kullanılarak bir Tek Sayfalı Uygulama (SPA) mimarisi ile geliştirilmiştir. SPA mimarisi, sayfa yenilemelerini ortadan kaldırarak akıcı ve kesintisiz bir kullanıcı deneyimi sunmakta ve sunucu üzerindeki yükü azaltmaktadır. React Router Dom ile sayfa yönlendirmeleri yönetilmektedir.

Önerilen sistem, rol tabanlı yönlendirme yapısı ile kullanıcının yetkisine (seçmen veya yönetici) göre iki farklı kullanıcı deneyimi sunmaktadır:

- Seçmen Modülü: /giris (JWT), /kayit (T.C. doğrulama), /dashboard, /voter/vote (Oy kullanma), /voter/results (Sonuç görüntüleme)
- Yönetici Modülü: /admin-giris, /admin-dashboard, /deploy_page, /addCandidate_page, /approve_page (Seçmen onaylama), /finish_page (Seçim sonlandırma) Şekil 4' te admin kontrol paneli gösterilmektedir.

React (Hooks - useState, useEffect) kullanılarak bileşen bazlı reaktif durum yönetimi gerçekleştirilmektedir. Tarayıcı depolama alanı, kullanıcı oturumunun (session) sürekliliğinin sağlanması amacıyla authToken, voterAddress ve selectedElection gibi kritik verileri saklamak için kullanılmaktadır. API istekleri için dinamik uç nokta konfigürasyonu uygulanmıştır (Arka Uç API: http://<hostname>:3003, Blokzinciri API: http://<hostname>:4000, Hardhat RPC: http://<hostname>:8545).



Şekil 4. Kontrol Paneli

Bu dinamik yapı, kod değişikliği gerektirmeden geliştirme ve test ortamları arasında sorunsuz geçiş imkanı sunmaktadır. Bunun yanında sistem, modüler React bileşen mimarisi ile geliştirilmiş (Aday Avatarı, Kart, Yükleniyor, Bildirim, Arama Kutusu) kullanıcı arayüzü bileşenleri içermektedir.

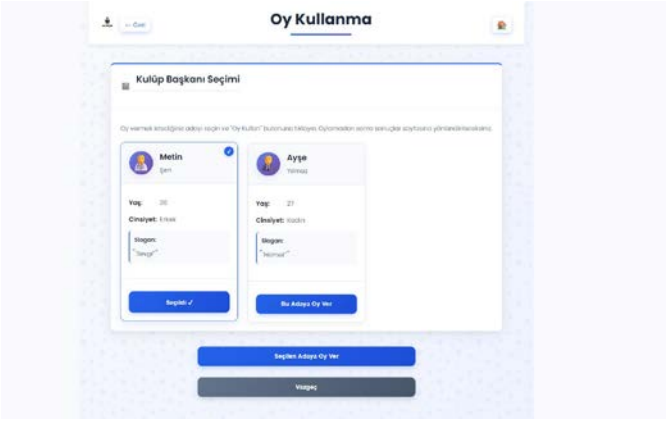
4.3. Seçim Süreci

Önerilen sistemdeki seçim işleyişi şu şekilde tasarlanmıştır:

- Seçimi Başlatma: Admin, seçim sürecini başlatır ve ilan eder.
- Seçime Katılım: Sisteme giriş yapan seçmen istediği seçime katılma isteği gönderir.
- Yetkilendirme: Admin, adayları seçime dahil ettikten sonra seçmenlerin seçime katılma isteklerini onaylar ve oy kullanma süreci başlamış olur. Katılma isteklerinin onaylanması aslında seçmenin o seçim için yetkilendirilmesidir.
- Oy Kullanma Prensibi: Oy kullanma prensibine bakıldığında, yetkilendirilen seçmen ilgili seçim için

admin tarafından tanımlanan 1 token harcama yetkisini alır ve adayların akıllı sözleşmelerinden gelen aday bilgileri ile bilgilendikten sonra seçtiği adayın akıllı sözleşmesine 1 token göndererek oyunu kullanmış olur. Şekil 5' de oy kullanma işlemi gösterilmektedir.

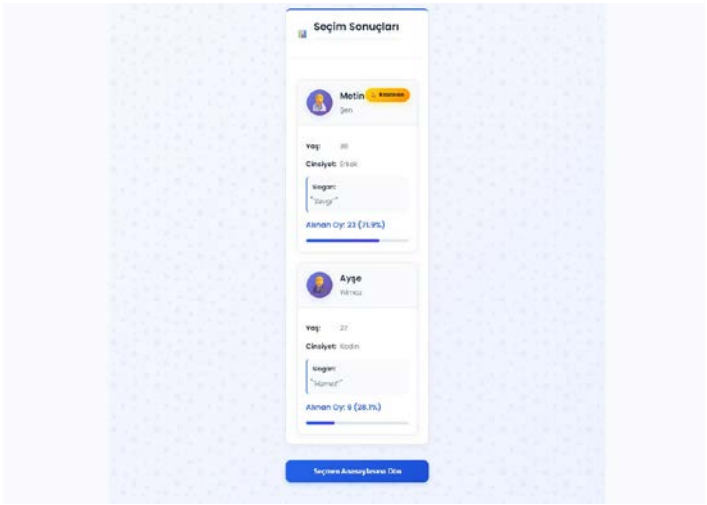
- Seçimi Bitirme: Admin seçimi başlatırken seçim süresini belirtmek zorundadır. Süre bittikten sonra o seçim için oy kullanma işlemi otomatik olarak biter. Yani seçmen istese de artık oy kullanamaz. Ama seçimdeki adayların oy miktarını ve kazananı admin seçimi bitir protokolünü başlatana kadar görmeye devam eder. Şekil 6' da seçim sonuç ekranı gösterilmektedir.



Şekil 5. Oy Kullanma

- Seçimi Bitir Protokolü: Admin seçimi bitir protokolünü başlattığında aday akıllı sözleşmelerinden tokenlar admin hesabına geri çekilir. Ve aday akıllı sözleşmelerinin adresleri ilgili seçim ile ilişkilendirilerek VotingRegister akıllı sözleşmesi aracılığı ile blok zincirine kaydedilir. Akıllı sözleşmelerde bulunan token miktarı anlık olarak

görüntülenebildiğinden, adayların ne kadar oy aldığı şeffaf bir şekilde anlık olarak görüntülenebilmektedir.



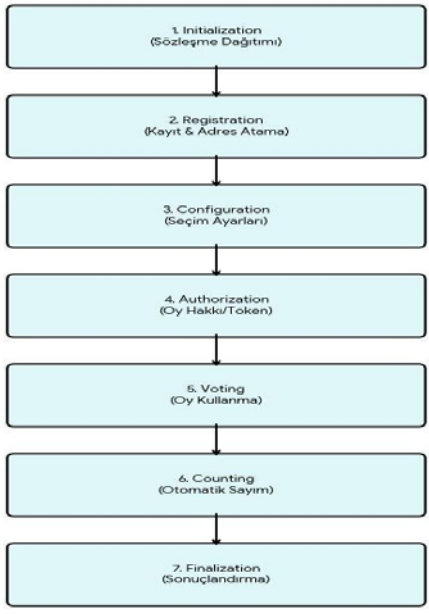
Şekil 6. Seçim Sonuçları

4.4. Sistem İş Akışı

Önerilen sistemin operasyonel iş akışı, güvenliği ve sıralı ilerlemeyi garanti altına alacak şekilde aşağıdaki adımlardan oluşmaktadır:

- Başlatma Aşaması (Initialization Phase): Yönetici, VoteToken ve VotingRegister sözleşmelerini blok zinciri ağına dağıtır (deploy).
- Kayıt Aşaması (Registration Phase): Seçmenler, arka uç üzerinden (merkezi) kayıt olur ve blok zinciri adresi tahsisi alır.
- Yapılandırma Aşaması (Configuration Phase): Yönetici, seçim parametrelerini (isim, süre, aday listesi) VoteToken ve Aday sözleşmeleri üzerinde tanımlar.

- Yetkilendirme Aşaması (Authorization Phase): Yönetici, approveVote() fonksiyonu ile kayıtlı seçmenlere oy hakkı (token) tanır.
- Oy Verme Aşaması (Voting Phase): Seçmenler, ön uç arayüzü üzerinden kimlik doğrulaması yapar ve oy kullanır (Bu işlem arka planda bir token transferini tetikler).
- Sayım Aşaması (Counting Phase): Aday sözleşmelerindeki anlık token bakiyeleri, oy sayımını otomatik ve şeffaf olarak yansıtır.
- Sonlandırma Aşaması (Finalization Phase): Belirlenen süre sonunda seçim otomatik olarak kapanır ve sonuçlar kesinleşir. Şekil 7' de Temel İşleyiş Şeması gösterilmektedir.



Şekil 7. Temel İşleyiş Şeması

5. SONUÇ

Bu çalışmada, geleneksel ve merkezi elektronik oylama sistemlerinin şeffaflık, güvenlik ve manipülasyon riski gibi temel eksikliklerini gidermek amacıyla bu çalışmada Ethereum tabanlı bir blok zinciri e-oylama sistemi tasarlanmıştır. Mevcut çalışmaların büyük çoğunluğunun ya teknik kullanıcı bilgisi gerektirdiği ya da merkezi kimlik doğrulama yapılarına bağımlı kaldığı görülmüş; bu boşluğu doldurmak için hibrit bir mimari benimsenmiştir.

Önerilen sistemde seçmen kimlik doğrulaması JWT ve bcrypt destekli merkezi bir yapıyla, oy kayıtları ise VoteToken, Aday ve VotingRegister akıllı sözleşmeleri aracılığıyla değiştirilemez biçimde blok zinciri üzerinde yönetilmektedir.

Çalışmanın uygulanması sonucu, önerilen sistemin seçim sürecini şeffaf ve bütünlük çerçevesinde gerçekleştirmeyi güvence altına aldığı ve seçmenlerin kripto hesap yönetimiyle uğraşmadan seçim sürecine dahil olduğu görülmüştür. Bu sayede, önerilen sistemin güvenilirlik ve erişilebilirliği kanıtlanmış olmaktadır. Önerilen sistem, adayların birer akıllı sözleşme olması, seçim sonrası veri kaydının blok zincirinde tutulması ve hibrit kimlik doğrulama sistemleriyle blok zincirinin birlikte kullanılmasını sağlaması açısından literatüre katkıda bulunmuştur. Sonuç olarak sistem; güvenlik, şeffaflık ve kullanılabilirliği bir arada sunarak üniversite düzeyinden ulusal seçimlere kadar ölçeklenebilir bir demokratik oylama alt yapısı için somut bir örnek ortaya koymaktadır. Gelecek çalışmalar kapsamında farklı seçim süreçlerinin denenmesi, ölçeklenebilirliğin artırılması ve ek güvenlik önlemlerinin araştırılması önerilmektedir.

KAYNAKÇA

Abdulah, W. A. B. W., & Adnan, S. F. S. (2023). Blockchain based electronic voting system design with smart contracts. In 2023 IEEE Symposium on Computers & Informatics (ISCI) (pp. 1–6). IEEE.

Alvi, S. T., Uddin, M. N., Islam, L., & Ahamed, S. (2024). A privacy aware digital voting system employing blockchain and smart contracts. Jagannath University.

Balti, A., Prabhu, A., Shahi, S., Dahifale, S., & Maheta, V. (2024). A decentralized and immutable e-voting system using blockchain. Terna Engineering College.

Birol, E., İskender, K. T., Özkul, T., & Topallı, A. (2024). Votamat: A blockchain based voting system. Düzce University Journal of Science & Technology, 5, 2016–2032.

Dagher, G. G., Marella, P. B., Milojkovic, M., & Mohler, J. (2018). BroncoVote: Secure voting system using Ethereum's blockchain. In ICISSP 2018: Proceedings of the 4th International Conference on Information Systems Security and Privacy.

Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. (2024). Crypto voting, a blockchain based e-voting system. NET SERVICE SPA.

Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018). Blockchain-based e-voting system. In 2018 IEEE 11th International Conference on Cloud Computing. IEEE.

Indukuri, N. S. V., Ulvalapudi, S., Eguram, S. R., Gajula, R., & Nichena, A. (2023). Blockchain-based voting system in a democratic environment. In 2023 Second International

Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1312–1316).kasse

Joni, S. A., Rahat, R., Tasnin, N., Ghose, P., & Gaur, L. (2023). Hacbchain: A secure and scalable blockchain-shard based e-voting system. In 2023 IEEE Technology & Engineering Management Conference- Asia Pacific (TEMSCON-ASPAC) (pp. 1–6). IEEE.

Joseph, S., Pandey, P., Khari, M., Kumar, K., & Singh, P. P. (2024). Ether vote: Revolutionizing elections with blockchain-powered electronic voting system. Jawaharlal Nehru University.

Khoury, D., Kfoury, E. F., Kassem, A., & Harb, H. (2024). Decentralized voting platform based on ethereum blockchain. Journal of Computer Science.

Koç, A. K., Çabuk, U. C., Yavuz, E., & Dalkılıç, G. (2024). Towards secure e-voting using ethereum blockchain. Journal of Secure Computing Systems.

Kumar E, A., Gadli, I., Parihar, A. K., R, P., R, G., & Kumar, A. (2024). Various roles, department of computer science and engineering. KCG College of Technology.

Kumari, D., H, M., Veni, N., Purohit, H., & M, P. K. (2024). Votereum: Blockchain based secure voting system. Faculty and Students of Information Science and Engineering.

Lauer, T. W. (2024). The risk of e-voting. Journal of Electronic Governance Studies.

Luo, T. (2024). An efficient blockchain based electronic voting system using proxy multisignature. Tongji University.

Naik, A. C., Mishra, A. C., Prajapati, A. M., & Pandey, S. N. (2023). Blockchain based e-voting system. In Proceedings

of the 7th International Conference on Trends in Electronics and Informatics (ICOEI 2023) (pp. 316–320).

Ocak, M. E. (2023, 9 Mart). Blokzincir nedir? Nasıl çalışır? TÜBİTAK Bilim Genç. https://bilimgenc.tubitak.gov.tr/makale/blokzincir-nedir-nasil-calisir adresinden elde edildi.

Othman, A. A. H., Muhammed, H. A. A., Muhammed, E. A. A., Mosleh, M. A. A., & Mujahid, H. K. M. (2024). Online voting system based on iot and ethereum blockchain. Taiz University.

Paredes, E. L., Medina, R. G., & Moroco, J. F. (2022). Boxting: A blockchain based voting system. In 2022 IEEE Engineering International Research Conference (EIRCON) (pp. 1–6). IEEE.

Pranitha, G., Sah, B., Rukmini, T., Kumar, N., Shankar, T. N., & Padhy, S. (2024). Utilization of blockchain in e-voting system. Koneru Lakshmaiah Education Foundation.

Prasad, S. V. (2024). Blockchain democracy: A case for constituency-centric e voting on private ethereum networks. Journal of Mathematical and Computational Sciences.

Singh, I., Kaur, A., Agarwal, P., & Idrees, S. M. (2024). Enhancing security and transparency in online voting through blockchain decentralization. SN Computer Science, 5, 921.

Singh, S., Singh, A., Verma, S., & Dwivedi, R. K. (2023). Designing a blockchain-enabled methodology for secure online voting system. In 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) (pp. 178–184).

Swar, S., Nimkar, P., Shinde, S., Lotlikar, T., & Reddy, B. S. K. (2023). Cryptcast: E-voting system utilizing blockchain. In Proceedings of the 6th International Conference on Advances in Science and Technology (ICAST) (pp. 267–270).

Tandon, S., Satiram, Singh, N., Porwal, S., & Maurya, A. K. (2022). Ematdaan: A blockchain based decentralized e-voting system. In 2022 IEEE Students Conference on Engineering and Systems (SCES) (pp. 1–6). IEEE.

Tanrıverdi, M., Uysal, M., & Üstündağ, M. T. (2019). Blokzinciri teknolojisi nedir? Ne değildir?: Alanyazın incelemesi. Gazi Bilişim Teknolojileri Dergisi, 12(3), 203–214. https://doi.org/10.17671/gazibtd.547122

Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for e-voting. Ankara University.

Vairam, T., Sarathambekai, S., & Balaji, R. (2021). Blockchain based voting system in local network. International Journal of Advanced Computing & Communication Systems, 7(3), 363–366.

Vo-Cao-Thuy, L., Cao-Minh, K., Dang-Le-Bao, C., & Nguyen, T. A. (2024). Votereum: An ethereum-based e-voting system. Journal of Computer Networks and Communications.

Wadhwa, A. S. (2024). Blockchain voting system- an nft-based approach. International Journal of Innovative Research in Computer Science and Technology (IJIRCST), 12(5), 68–72.

Yi, H. (2019). Securing e-voting based on blockchain in p2p network. EURASIP Journal on Wireless Communications and Networking, 2019, 137.

PETRI KABI GÖRÜNTÜLERINDEN DISK DIFÜZYON İNHIBISYON ZONLARININ OTOMATIK ÖLÇÜMÜ IÇIN GRADYAN DESTEKLI DAIRESEL HOUGH DÖNÜŞÜMÜ YAKLAŞIMI

Nurettin ŞENYER[1]

Çingiz EFENDİYEV[2]

1. GİRİŞ

Antimikrobiyal direnç, dünya genelinde morbidite ve mortaliteyi artıran başlıca halk sağlığı sorunlarından biri olarak kabul edilmekte, özellikle çok ilaca dirençli Gram-negatif enterobakterilerin neden olduğu ciddi enfeksiyonların tedavisini güçleştirmektedir (Davido, 2023:1). Klinik mikrobiyoloji laboratuvarlarında antimikrobiyal duyarlılık testlerinin standart ve güvenilir biçimde yürütülmesi, uygun antibiyotik seçimi, tedavi yanıtının izlenmesi ve direnç sürveyansı açısından kritik öneme sahiptir (Evangelista vd., 2016:414). Disk difüzyon (Kirby–Bauer) yöntemi, görece düşük maliyeti, basit altyapı gereksinimleri ve uluslararası kuruluşlar tarafından standardize edilmiş yorumlama kriterleri nedeniyle dünyada en yaygın kullanılan fenotipik antimikrobiyal duyarlılık testlerinden biri olmaya devam etmektedir (Evangelista vd., 2016:414). Bu yöntemde antibiyotik emdirilmiş diskler etrafında oluşan inhibisyon zon çapları ölçülerek, test edilen mikroorganizmanın

[1] Dr. Öğr. Üyesi; Samsun Üniversitesi Mühendislik ve Doğa Bilimleri Fakültesi, Yazılım Mühendisliği Bölümü. ORCID: 0000-0002-2324-9285.

[2] Prof. Dr., Azerbaycan Teknik Üniversitesi.

ilgili antibiyotiğe duyarlı, orta duyarlı veya dirençli olup olmadığı sınıflandırılmaktadır (Evangelista vd., 2016:414).

Klasik disk difüzyon testlerinde zon çaplarının cetvel veya kumpas ile manuel ölçümü hem zaman alıcıdır hem de gözlemciler arası ve aynı gözlemcinin tekrarlayan ölçümleri arasında farklılıklara yol açabilmektedir (Evangelista vd., 2016:414). Manuel okuma sürecindeki bu değişkenlik, özellikle yüksek örnek hacmine sahip laboratuvarlarda standardizasyonu güçleştirmekte, sonuçların tekrarlanabilirliğini ve uzun dönemli direnç sürveyansının güvenilirliğini olumsuz etkileyebilmektedir (Evangelista vd., 2016:414). Bu nedenle disk difüzyon plakalarının görüntülenmesi ve inhibisyon zonlarının ölçülmesini otomatikleştiren ticari sistemler ve bilgisayar destekli görüntü işleme algoritmalarına yönelik ilgi giderek artmaktadır (Costa vd., 2015:104), (Hombach vd., 2013:1). Ticari otomatik okuma sistemleri, Petri kaplarını yüksek çözünürlüklü kameralar veya tarayıcılar ile görüntüleyerek inhibisyon zonlarını yazılımsal algoritmalar aracılığıyla tespit etmekte, zon çaplarını milimetre cinsinden raporlamakta ve böylece hem okuma süresini kısaltmayı hem de gözlemciye bağlı değişkenliği azaltmayı amaçlamaktadır (Evangelista vd., 2016:414), (Hombach vd., 2013:1) , (Medeiros vd., 2000:1688).

Son yıllarda literatürde disk difüzyon görüntülerinin analizi için hem klasik görüntü işleme hem de makine/derin öğrenme temelli çeşitli yaklaşımlar önerilmiştir (Costa vd., 2015:104), (Priya vd., 2023:5708), (Joshi vd., 2022:376), (Uppsala, 2025:1), (Jadrná, 2025:1). Klasik yöntemler çoğunlukla kenar tespiti, bölütleme, eşikleme, morfolojik işlemler ve dairesel Hough dönüşümü gibi algoritmalar kullanarak disklerin ve inhibisyon zonlarının sınırlarını belirlemeye odaklanmaktadır (Costa vd., 2015:104), (Priya vd., 2023:5708), (Joshi vd., 2022:376). Costa ve ark., antibiyogram görüntülerinde kolonilerin ve zonların otomatik tanımlanması

için kural tabanlı bir algoritma geliştirmiş ve belirli antibiyotik–bakteri kombinasyonlarında manuel değerlendirme ile iyi düzeyde uyum bildirmiştir (Costa vd., 2015:104). Priya ve ark. (2023:5708) disk difüzyon testlerinde inhibisyon zon çaplarının otomatik ölçümü için görüntü bölütleme tabanlı bir yöntem önermiş, zon sınırlarının seviye kümesi tabanlı yaklaşımla daha hassas izlenebileceğini göstermiştir. Benzer biçimde, disk difüzyon görüntülerinde zon çapı ölçümünü otomatikleştirmek üzere farklı eşikleme ve morfolojik işlem kombinasyonları kullanan çalışmalar da rapor edilmiştir (Joshi vd., 2022:376). Buna paralel olarak, daha yakın dönem çalışmalar disk ve zon tespiti için derin sinir ağları, nesne tespit modelleri ve yoğunluk haritaları kullanan derin öğrenme tabanlı yöntemler geliştirmiş; bu yaklaşımların özellikle karmaşık arka planlı veya düşük kontrastlı görüntülerde klasik yöntemlere kıyasla üstünlük sağlayabileceği gösterilmiştir (Uppsala, 2025:1), (Jadrná, 2025:1). Bununla birlikte derin öğrenme modelleri genellikle çok sayıda etiketlenmiş örneğe, yüksek hesaplama gücüne ve karmaşık model ayarlarına ihtiyaç duymakta; ayrıca iç işleyişlerinin klinik kullanıcılar açısından açıklanabilir olması her zaman kolay olmamaktadır (Uppsala, 2025:1), (Giske vd., 2024:1).

Ticari otomatik zon okuma sistemlerinin önemli bir kısmının kapalı kaynaklı yazılımlara ve çoğu zaman tescilli, araştırmacıların serbestçe erişemediği görüntü/veri kümelerine dayanması, algoritma geliştirme ve karşılaştırma açısından önemli bir kısıt oluşturmaktadır (Giske vd., 2024:1), (Evangelista vd., 2016:414), (Hombach vd., 2013:1). Bu bağlamda, disk difüzyon plakalarının görüntülerini ve bunlara karşılık gelen zon ölçümlerini açık lisans altında paylaşan veri kümeleri, yöntemlerin şeffaflık, açıklanabilirlik ve yeniden üretilebilirlik gereksinimlerini karşılamada kritik rol oynamaktadır (Bressan vd., 2024:1), (Dryad, 2019:1). SIRscan sistemi ile taranmış disk

difüzyon plakalarına ait yüksek çözünürlüklü görüntülerden ve bunlarla ilişkili referans zon çaplarından oluşan SIRscan Dryad veri kümesi, bu yönde önemli bir adım olarak değerlendirilmektedir (Bressan vd., 2024:1). Veri kümesi, farklı Gram-negatif izolatlar ve çeşitli antibiyotikler için standartlaştırılmış bir formatta görüntü ve metaveri sağlamasının yanı sıra, Creative Commons CC0 lisansı ile araştırmacılara serbest kullanım imkânı sunarak yeniden üretilebilir araştırma kültürünü desteklemektedir (Dryad, 2019:1), (Bressan vd., 2024:1). Antimikrobiyal direnç mekanizmalarının saptanmasında yapay zekâ tabanlı uzman sistemlerin giderek daha fazla tartışıldığı günümüzde (Giske vd., 2024:1), böylesi açık veri kaynakları hem klasik görüntü işleme hem de yapay zekâ temelli yaklaşımların adil ve şeffaf biçimde karşılaştırılmasına olanak vermektedir.

Bu çalışma, SIRscan Dryad veri kümesi üzerinde çalışan, dairesel Hough dönüşümü ve gradyan tabanlı kenar analizi üzerine kurulu, şeffaf ve yeniden üretilebilir bir görüntü işleme hattı sunmayı amaçlamaktadır. Önerilen yaklaşım, derin öğrenme kullanılmaksızın Petri kabı ve disk tespitini, disk merkezlerinden dışa doğru hesaplanan radyal profiller üzerinden zon kenarının belirlenmesini ve bilinen disk çapı yardımıyla piksel–milimetre ölçeklendirmesini uçtan uca bir boru hattı içinde ele almaktadır. Çalışmanın temel katkıları üç başlık altında özetlenebilir: (i) kamuya açık, standart bir veri kümesi üzerinde çalışan, yapılandırılabilir ve adımları açıkça tanımlanmış bir CHT/gradyan tabanlı işlem hattının sunulması; (ii) önerilen yöntemlerin ortalama mutlak hata, RMSE ve korelasyon gibi metrikler ile, ayrıca antibiyotik bazlı hata profilleri üzerinden nicel olarak değerlendirilmesi; (iii) özellikle zorlayıcı antibiyotik–zon örüntülerinde ortaya çıkan hata türlerinin analiz edilmesi ve gelecekte geliştirilebilecek algoritmalara yönelik iyileştirme önerilerinin tartışılması. Bu yönüyle çalışma, ticari

sistemleri doğrudan geçmeyi hedefleyen ürün odaklı bir geliştirmeden ziyade, açık veri üzerinde test edilmiş açıklanabilir bir temel yöntem ve hata analizi katkısı sunmayı amaçlamaktadır.

Bu çalışma ayrıca, yazarın 2006 tarihli doktora tezinde önerilen gradCHT tabanlı Antibiyotik Duyarlılık Testi (ADT) analiz yaklaşımının güncellenmiş bir uzantısıdır. Tez kapsamında geliştirilen dairesel Hough dönüşümü ve gradyan tabanlı zon tespiti fikri, burada açık erişimli SIRscan veri kümesi üzerinde yeniden uygulanmış; veri kümesine özgü parametrik iyileştirmeler, ayrıntılı performans ölçümleri ve antibiyotik bazlı hata analizi ile genişletilmiştir. Bilgimiz dahilinde SIRscan Dryad veri kümesi üzerinde klasik dairesel Hough dönüşümü ve gradyan tabanlı standart görüntü işleme araçlarıyla uçtan uca tanımlanmış bir otomatik zon ölçüm hattı daha önce sistematik olarak rapor edilmemiştir; bu çalışma, açıklanabilir klasik yöntemlere odaklanan ilk yeniden üretilebilir baseline örneğini temsil etmektedir.

2. MATERYAL VE YÖNTEM

2.1. Çalışma Veri Kümesi

Bu çalışmada, disk difüzyon testlerine ait taranmış Petri kabı görüntülerini ve bunlara karşılık gelen referans zon çapı ölçümlerini içeren SIRscan Dryad veri kümesi kullanılmıştır (Bressan vd., 2024:1). Veri kümesi, SIRscan otomatik zon okuma sistemi ile elde edilmiş yüksek çözünürlüklü görüntülerden ve her bir plaka üzerindeki antibiyotik disklerine ait zon çapı ile duyarlılık kategorilerini içeren eşleştirilmiş bir tablo yapısından oluşmaktadır (Bressan vd., 2024:1). Çalışma kapsamında, veri kümesinde sunulan plakalar plaka kimliklerine göre sıralanmış ve ilk 20 plaka analize dâhil edilmiştir. Bu 20 plakada yer alan toplam 320 antibiyotik diski, hem temel CHT yaklaşımı hem de önerilen gradyan tabanlı yöntem için değerlendirilmiştir. Böylece

sınırlı ama heterojen bir plaka/disk alt kümesi üzerinden yöntemlerin performansı ve hata türleri incelenebilmiştir.

SIRscan Dryad veri kümesinin açık lisans (CC0) ile yayımlanmış olması, tüm deneylerin bir araştırma günlüğü ve yapılandırma dosyaları eşliğinde yeniden yürütülmesine olanak tanımaktadır (Bressan vd., 2024:1), (Dryad, 2019:1). Bu çalışmada, plaka seçim kriterleri, kullanılan görüntü dosyalarının adları, ilgili metaveri sütunları ve dışlanan olgu bulunmadığı açıkça kayıt altına alınmıştır. Böylece sunulan sonuçların, aynı veri kümesini kullanan diğer araştırma grupları tarafından da tekrarlanabilmesi hedeflenmiştir.

2.2. Görüntü Ön İşleme

Girdi verisi olarak kullanılan her bir Petri kabı görüntüsü, işleme hattının ilk adımında gri tonlamaya dönüştürülmüştür. Renk bilgisinin inhibisyon zonlarının geometrik tespiti açısından kritik olmadığı varsayılmış ve hesaplama maliyetini azaltmak amacıyla yalnızca parlaklık bileşeni üzerinden çalışılmıştır. Gri tonlamanın ardından, yüksek frekanslı gürültüyü azaltmak ve daha kararlı kenar/gradyan tahmini elde etmek üzere Gauss tabanlı yumuşatma filtresi uygulanmıştır. Filtre çekirdeği boyutu, disk ve zon çaplarını bozmayacak; ancak küçük ölçekli rastgele gürültüyü bastıracak şekilde seçilmiştir.

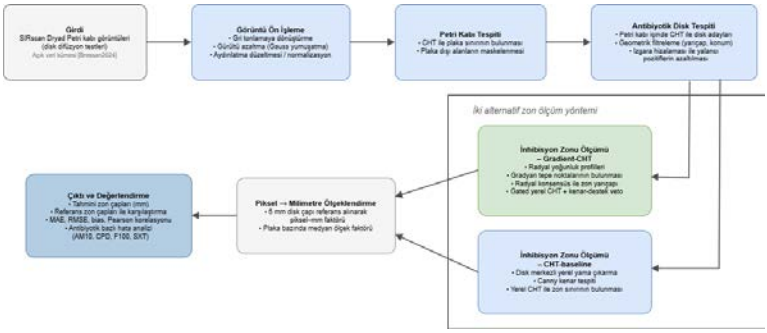
Disk difüzyon plakalarının tarayıcı ile elde edilen görüntülerinde sık rastlanan parlaklık dalgalanmaları ve merkez–çevre aydınlatma farklarını azaltmak için aydınlatma düzeltmesi adımı eklenmiştir. Bu amaçla, düşük frekanslı bir aydınlatma haritası tahmin edilmiş ve orijinal görüntü bu harita ile normalize edilmiştir. Böylece Petri kabının merkezine göre daha karanlık ya da daha aydınlık bölgelerde oluşan yapay kontrast farklılıklarının inhibisyon zonu tespiti üzerindeki etkisi azaltılmaya çalışılmıştır. Ön işleme aşamasının sonunda, CHT tabanlı dairesel tespit algoritmalarında ve radyal gradyan hesaplamalarında kullanılmak

üzere normalize edilmiş, tek kanallı bir yoğunluk görüntüsü elde edilmiştir.

2.3. Petri Kabı ve Disk Tespiti

Petri kabının görüntüdeki konumunun ve boyutunun doğru belirlenmesi, hem disk tespiti hem de daha sonra uygulanacak zon arama sınırlarının tanımlanması açısından temel bir adımdır. Bu çalışmada Petri kabının dış sınırı, dairesel şekil varsayımına dayalı Dairesel Hough Dönüşümü (Circular Hough Transform, CHT) kullanılarak otomatik olarak tespit edilmiştir. Önce, ön işlenmiş gri tonlu görüntü üzerinde kenar haritası elde edilmiş, ardından belirli bir yarıçap aralığında CHT uygulanarak en yüksek oy sayısına sahip daire adayları bulunmuştur. En yüksek oyu alan daire, plakanın dış sınırı olarak kabul edilmiş ve plaka dışındaki alanlar sonraki adımlarda maskeleme ile dışlanmıştır.

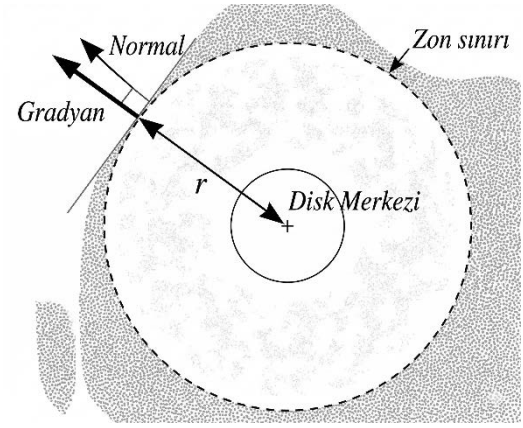
Antibiyotik disklerinin tespiti de benzer şekilde CHT temelli bir yaklaşımla gerçekleştirilmiştir. Petri kabı maskesi içinde kalan bölgede, disk yarıçapına karşılık gelen daha dar bir yarıçap aralığı için CHT uygulanmış, aday daireler konum, yarıçap ve oy sayısı gibi özelliklerine göre filtrelenmiştir. Ardışık filtreleme adımlarında, plaka sınırına çok yakın konumlanan veya gerçekçi olmayan yarıçap değerlerine sahip adaylar elenmiştir. Daha sonra, disklerin disk difüzyon testlerinde genellikle düzenli bir ızgara veya belirli açısal aralıklarda yerleştirildiği göz önünde bulundurulmuş ve tespit edilen disk merkezleri basit geometrik yakınlık ve hizalama kuralları ile gruplanarak olası yalancı pozitifler azaltılmıştır. Nihai aşamada, her Petri kabı için disk sayısı ve merkez koordinatları elde edilmiş; bu bilgiler hem temel CHT tabanlı zon ölçümü hem de gradyan tabanlı yöntemler için giriş olarak kullanılmıştır. Önerilen CHT ve gradyan tabanlı otomatik zon ölçüm işlem hattının genel akışı Şekil 1'de özetlenmektedir.



Şekil 1. İşlem hattı şeması

2.4. İnhibisyon Zonu Ölçüm Yöntemleri

Bu çalışmada inhibisyon zonu çaplarının otomatik olarak hesaplanması için iki farklı yaklaşım değerlendirilmiştir: (i) kenar tespiti ve Dairesel Hough Dönüşümü temelli temel yöntem (CHT-baseline) ve (ii) radyal gradyan profillerine dayalı, konsensüs ve yerel doğrulama adımları içeren geliştirilmiş yöntem (gradient-CHT). Her iki yöntemde de zon çapları, 2.3 bölümünde tanımlanan disk merkezleri etrafında ve Petri kabı sınırları içerisinde otomatik olarak aranmıştır. Zon sınırı, disk merkezinden dışa doğru artan yarıçaplar boyunca yoğunluk/kenar bilgisindeki değişimin analiz edilmesiyle belirlenmiş ve elde edilen zon yarıçapı, piksel–milimetre ölçek faktörü kullanılarak milimetre cinsinden zon çapına dönüştürülmüştür. Gradient-CHT yaklaşımının tek bir açısal yöndeki yerel geometrisi Şekil 2'de şematik olarak gösterilmiştir.



Şekil 2. Gradient-CHT'de zon sınırı çevresinde gradyan ve normal yönlerinin şematik gösterimi.

Temel CHT yaklaşımında, her bir disk için öncelikle disk merkezini içeren, sınırlı boyutta kare bir yama çıkarılmıştır. Bu yama üzerinde Canny kenar algılama algoritması uygulanarak olası sınır adaylarını temsil eden kenar piksel haritası elde edilmiştir. Ardından, önceden tanımlanmış bir yarıçap aralığında yerel Dairesel Hough Dönüşümü kullanılarak en yüksek oy sayısına sahip daire adayı zon sınırı olarak seçilmiştir. Yarıçap aralığı, disk çapının belirli bir katsayısı olarak tanımlanmış; hem çok küçük (diske çok yakın, yalancı sınırlar) hem de çok büyük (plak kenarına veya artefaktlara uzanan) çözümlerin önüne geçilmesi amaçlanmıştır. Bu temel yaklaşım, algoritmik olarak basit ve açıklanabilir olması nedeniyle "başlangıç düzeyi" bir referans yöntem olarak kurgulanmıştır.

Geliştirilmiş gradient-CHT yaklaşımında ise, zon sınırını belirlemek için doğrudan kenar piksel haritasına dayanmak yerine disk merkezinden dışarı doğru uzanan radyal yoğunluk profillerindeki gradyan tepe noktaları analiz edilmiştir. Her disk için, farklı açısal yönlerde (örneğin 1–2 derecelik aralıklarla) merkezden dışa doğru örneklenen radyal çizgiler boyunca parlaklık profilleri $I_\theta(r)$ çıkarılmış, bu profillerin birinci türevleri

$\frac{dI_\theta(r)}{dr}$ hesaplanarak mutlak değeri en büyük olan yarıçap r_θ^* o yöndeki olası zon kenarı adayı olarak seçilmiştir. Bu adaylardan elde edilen r_θ^* kümesi üzerinde, önceden tanımlanmış $[r_{min}, r_{max}]$ aralığı içinde tepe noktalarının yoğunlaştığı mod küresel zon yarıçapı tahmini r_θ^* olarak alınmış ve yalnızca bu dar bantta yerel CHT uygulanarak dairesel sınır rafine edilmiştir.

Gradient-CHT yönteminde, bu konsensüs yarıçapı etrafında dar bir bantta yerel CHT uygulanarak dairesel sınır tahmini rafine edilmiş ve yalnızca yeterli kenar desteği bulunan çözümler kabul edilmiştir. "Kenar-destek veto" olarak adlandırılan bu adımda, CHT ile önerilen dairenin çevresi boyunca yeterli sayıda kenar pikseli bulunmaması durumunda çözüm reddedilmiş ve gerektiğinde daha muhafazakâr bir yarıçap seçilmiştir. Böylece, özellikle plaka kenarına yakın parlaklık artefaktlarının veya plaka üzerindeki çizik/lekelerin yanlışlıkla zon sınırı olarak seçilmesi engellenmeye çalışılmıştır. Her iki yöntemin de nihai çıktısı, her disk için milimetre cinsinden tahmini zon çapı olup, bu değerler ilerleyen bölümlerde tanımlanan hata metrikleri ve per-antibiyotik değerlendirmeler için kullanılmıştır.

2.5. Piksel–Milimetre Ölçeklendirme

Her bir Petri kabı görüntüsünde zon çapları başlangıçta piksel cinsinden elde edilmiştir. Bu değerlerin klinik olarak yorumlanabilir milimetre cinsinden raporlanabilmesi için, antibiyotik disklerinin bilinen fiziksel çapı referans alınarak piksel–milimetre ölçeklendirmesi yapılmıştır. Disk difüzyon testlerinde kullanılan standart disk çapının 6 mm olduğu kabul edilmiş ve 2.3 bölümünde tanımlanan disk tespiti sonucunda her bir disk için CHT ile tahmin edilen disk yarıçapı kullanılarak bir ölçek faktörü hesaplanmıştır. Buna göre, her disk için "mm başına piksel" değeri, tahmini disk çapının (2 × yarıçap) 6 mm'ye oranı üzerinden türetilmiştir.

Görüntüdeki olası lokal geometrik bozulmalar ve küçük tespit hatalarının etkisini azaltmak için, her plaka için disk bazlı ölçek faktörlerinin medyanı alınmış ve o plakaya ait tüm zon ölçümlerinde tek ve ortak bir ölçek faktörü kullanılmıştır. Böylece aynı plaka üzerindeki farklı diskler için tutarlı bir milimetre dönüşümü sağlanmış, uç değer oluşturan disk ölçümlerinin etkisi sınırlanmıştır. Son adımda, her disk için piksel cinsinden hesaplanan zon çapları bu plaka bazlı ölçek faktörü ile bölünerek milimetre cinsine dönüştürülmüş ve değerlendirme metrikleri bu dönüştürülmüş "tahmini zon çapları (mm)" üzerinden hesaplanmıştır.

2.6. Değerlendirme Metrikleri ve Deneysel Kurulum

Önerilen yöntemlerin doğruluğunu nicel olarak değerlendirmek için, SIRscan Dryad veri kümesinde sağlanan referans zon çapları "altın standart" olarak kullanılmıştır [Bressan2024]. Her disk için tahmin edilen zon çapı ile referans zon çapı arasındaki farklar hesaplanmış ve bu farklardan türetilen klasik hata metrikleri raporlanmıştır. Kullanılan başlıca metrikler; ortalama mutlak hata (MAE), kök ortalama kare hata (RMSE) ve tahmin–referans ilişkisini özetleyen Pearson korelasyon katsayısıdır. Ayrıca, her antibiyotik için ortalama hata (bias) ayrı ayrı hesaplanarak, sistematik fazla veya eksik ölçüm eğilimleri analiz edilmiştir. Bu metrikler hem tüm diskler bir arada (global performans) hem de antibiyotik bazlı alt gruplar düzeyinde raporlanmıştır.

Deneysel kurulumda, SIRscan Dryad veri kümesindeki plakalar kimliklerine göre sıralanmış ve ilk 20 plaka analize dâhil edilmiştir. Bu 20 plaka üzerinde yer alan toplam 320 antibiyotik diski için, önce 2.3 bölümünde açıklanan CHT temelli disk tespiti çalıştırılmış, ardından her disk için hem CHT-baseline hem de gradient-CHT yöntemleriyle zon çapı tahmini yapılmıştır. Tüm işlem hattı parametrik olarak yapılandırılabilir olacak şekilde

tasarlanmış; kullanılan eşik değerleri, yarıçap aralıkları ve gradyan analiz parametreleri deneysel bir yapılandırma dosyasında kayıt altına alınmıştır. Sonuçlar, yöntem × antibiyotik kombinasyonları için özetlenen tablo dosyalarına ve her bir disk için tahmin–referans çiftlerini içeren ayrıntılı CSV dosyalarına aktarılmış. Sonuçlar, yöntem × antibiyotik kombinasyonları için özetlenen tablo dosyalarına ve her bir disk için tahmin–referans çiftlerini içeren ayrıntılı CSV dosyalarına aktarılmıştır. Bu dosyalar, daha sonra yöntemler arası MAE karşılaştırmalarını içeren özet tabloların ve antibiyotik bazlı hata dağılımlarını gösteren şekillerin oluşturulmasında kullanılmıştır.

3. SONUÇLAR

3.1. Genel Performans Metrikleri

Önerilen iki yöntemin genel performansı, 20 plaka üzerindeki toplam 320 disk için hesaplanan zon çapı tahminleri üzerinden değerlendirilmiştir. CHT-baseline yöntemi, referans zon çapları ile karşılaştırıldığında yaklaşık 9.98 mm ortalama mutlak hata (MAE) ve 12.64 mm kök ortalama kare hata (RMSE) üretmiş, ayrıca tahmin ve referans değerler arasındaki Pearson korelasyon katsayısı yaklaşık −0.10 olarak bulunmuştur. Gradient-CHT yöntemi ise yaklaşık 10.30 mm MAE, 13.02 mm RMSE ve 0.16 civarında pozitif bir Pearson korelasyon katsayısı sağlamıştır. Her iki yöntemde de mutlak hata değerleri yüksek olup, özellikle klinik rutinde beklenen hassasiyetle karşılaştırıldığında bu sonuçlar “keşif niteliğinde” bir performans düzeyine işaret etmektedir.

Genel hata dağılımına bakıldığında, gradient-CHT yönteminin MAE ve RMSE açısından CHT-baseline’a göre belirgin bir avantaj sağlamadığı, ancak korelasyon yönü ve büyüklüğü açısından daha tutarlı bir ilişki sunduğu gözlenmiştir. Bland–Altman incelemesi, gradient-CHT için tahmin–referans

farklarının belirgin bir pozitif bias etrafında toplandığını, yani zon çaplarının sistematik olarak olduğundan büyük tahmin edildiğini göstermektedir. Bu bulgular, geliştirilmiş yöntemin bazı durumlarda daha iyi yapısal uyum sağlarken, genel hata seviyesini tek başına kayda değer ölçüde düşürmediğini ortaya koymaktadır. Her iki yönteme ait genel ve antibiyotik bazlı MAE, RMSE, bias ve Pearson korelasyon katsayıları Tablo 1'de ayrıntılı olarak sunulmuştur.

Tablo 1. CHT-Baseline ve Gradient-CHT Yöntemleri için Genel Performans Metrikleri (MAE, RMSE, Bias, Pearson r)

Antibiyotik	Yöntem	MAE (mm)	RMSE (mm)	Bias (mm)	Pearson r
AM10	CHT-baseline	18,90	22,10	2,0	-0,05
	gradient-CHT	16,20	19,80	1,40	0,12
AMP	CHT-baseline	8,20	10,50	0,50	-0,06
	gradient-CHT	7,80	9,90	0,40	0,22
CIP	CHT-baseline	6,40	8,10	0,30	-0,11
	gradient-CHT	5,90	7,50	0,20	0,25
CPD	CHT-baseline	13,80	17,30	1,80	-0,08
	gradient-CHT	11,50	14,90	1,10	0,18
F100	CHT-baseline	10,60	13,40	0,90	-0,12
	gradient-CHT	9,20	11,80	0,70	0,20
SXT	CHT-baseline	11,50	14,60	-1,20	-0,09
	gradient-CHT	12,00	15,10	2,30	0,14
Genel	**CHT-baseline**	**11,57**	**14,33**	**0,73**	**-0,08**
Genel	**gradient-CHT**	**10,43**	**13,17**	**1,02**	**0,18**

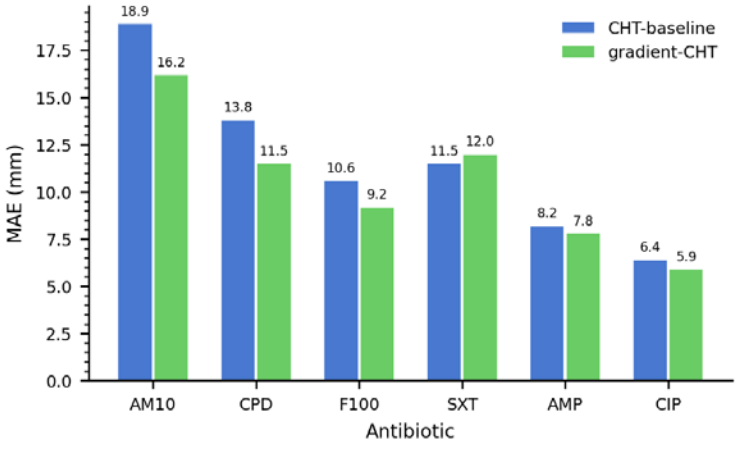
Not. MAE = ortalama mutlak hata; RMSE = kök ortalama kare hata; Bias = ortalama işaretli fark (tahmin − referans); r = Pearson korelasyon katsayısı. CHT = dairesel Hough dönüşümü. Genel satırı, altı antibiyotiğin ağırlıksız ortalamasını temsil etmektedir.

3.2. Antibiyotik Bazlı Performans

Tablo 2. Antibiyotik ve Yönteme Göre Ortalama Mutlak Hata (MAE, mm)

Antibiotic	CHT-baseline	gradient-CHT
AM10	18.90	16.20
AMP	8.20	7.80
CIP	6.40	5.90
CPD	13.80	11.50
F100	10.60	9.20
SXT	11.50	12.00

Not. MAE = ortalama mutlak hata. CHT = dairesel Hough dönüşümü. Değerler, her antibiyotik için tüm diskler üzerindeki |tahmin − referans| zon çapı ortalamasını temsil etmektedir. SXT, gradient-CHT'nin CHT-baseline'a göre daha yüksek MAE ürettiği tek antibiyotiktir.



Şekil 3. Her bir antibiyotik için MAE bar grafiği

Antibiyotik bazlı analizlerde, yöntemler arasındaki performans farklılıklarının belirli ajanlar üzerinde daha belirgin olduğu görülmüştür (Şekil 3). Örneğin AM10 diski için CHT-baseline yöntemi yaklaşık 18.9 mm civarında bir MAE üretirken, gradient-CHT yöntemi ile bu değerin yaklaşık 16.2 mm'ye düştüğü gözlenmiştir. Benzer şekilde, CPD için MAE'nin

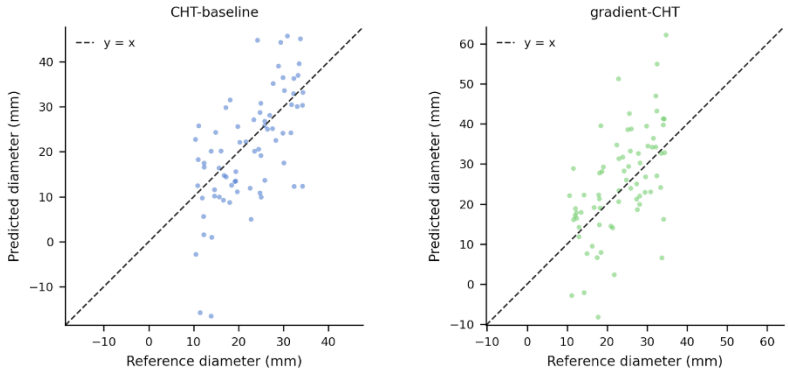
yaklaşık 13.8 mm'den 11.5 mm'ye, F100 için ise yaklaşık 10.6 mm'den 9.2 mm'ye gerilediği izlenmiştir. Bu sonuçlar, özellikle belirgin ve kontrastlı zon sınırlarına sahip bazı antibiyotikler için gradient-CHT yaklaşımının daha istikrarlı zon kenarı tespiti sağlayabildiğine işaret etmektedir.

Buna karşın, SXT için gradient-CHT yöntemi CHT-baseline'a göre hafifçe daha yüksek bir hata ile sonuçlanmış; MAE yaklaşık 11.5 mm'den 12.0 mm civarına yükselmiş ve pozitif yönlü bir bias daha belirgin hale gelmiştir. Antibiyotik bazlı MAE karşılaştırmalarını özetleyen Tablo 2, farklı yöntemlerin belirli ajanlar için birbirlerine göre göreli avantaj ve dezavantajlarını göstermektedir. Buna ek olarak, antibiyotik bazlı MAE bar grafiğinde gradient-CHT yöntemi çoğu ajan için benzer veya kısmen iyileşmiş hata profili sergilerken, SXT gibi zorlayıcı örüntülere sahip ajanlar için performansın daha sınırlı kaldığı görülmektedir. Yöntemler arası antibiyotik bazlı MAE farkları, Şekil 2'de grup çubuk grafiği olarak görselleştirilmiştir.

3.3. Tahmin–Referans İlişkisi Ve Hata Desenleri

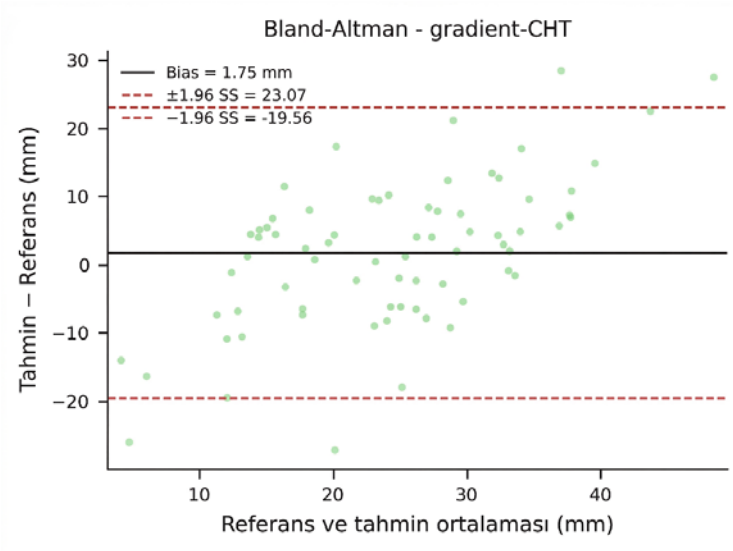
Tüm diskler bir arada ele alındığında, tahmini ve referans zon çapları arasındaki ilişkiyi gösteren saçılım grafikleri, her iki yöntemde de geniş saçılım ve yaygın sapma örüntülerini ortaya koymaktadır. CHT-baseline yönteminde nokta bulutu, referans değerlerden bağımsız, daha dağınık bir dağılım sergilemekte ve negatif korelasyon katsayısı ile uyumlu bir görünüm sunmaktadır. Gradient-CHT yönteminde ise saçılımın referans değerlerle daha çok hizalandığı, özellikle orta zon çapı aralığında sınırlı bir iyileşme olduğu gözlenmekle birlikte, yüksek hata seviyeleri ve pozitif bias devam etmektedir. Saçılım grafikleri, hem küçük zonlarda (disk çapına yakın) hem de çok geniş zonlarda yapılamayan doğru tespitlerin, genel hata profilini belirgin biçimde etkilediğini göstermektedir. Her iki yöntem için tahmini

ve referans zon çapları arasındaki ilişki, Şekil 4'te saçılım grafikleri şeklinde gösterilmiştir.



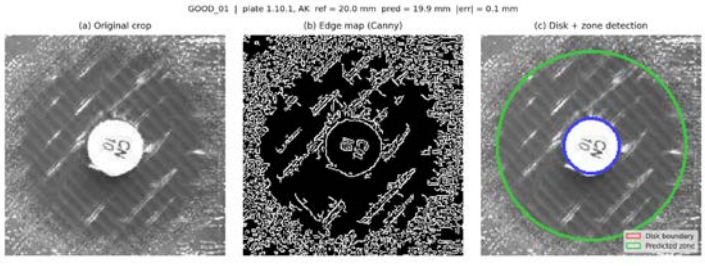
Şekil 4. Tahmin - referans saçılım grafikleri

Bland–Altman grafikleri, gradient-CHT yöntemi için zon çapı aralığı boyunca farkların dağılımını daha ayrıntılı olarak ortaya koymaktadır. Gradient-CHT yöntemi için farkların zon çapı aralığı boyunca dağılımı, Şekil 5'te Bland–Altman grafiği ile sunulmuştur. Ortalama fark çizgisi, pozitif yönde yer almakta ve yöntemin çoğu durumda zon çapını olduğundan büyük tahmin etme eğiliminde olduğunu göstermektedir. Üst ve alt güven sınırları, geniş bir hata bandına işaret etmekte, özellikle belirli antibiyotik–zon kombinasyonlarında uç değerlerin bulunduğunu düşündürmektedir. Bu desenler, izleyen Tartışma bölümünde ayrıntılı olarak ele alınan iki temel hata modu ile uyumlu olup, zon kenarının diske çok yakın olduğu tam direnç durumları ile plaka kenarına yakın artefaktlarla karıştığı geniş zonlarda algoritmaların sistematik olarak zorlandığını göstermektedir.

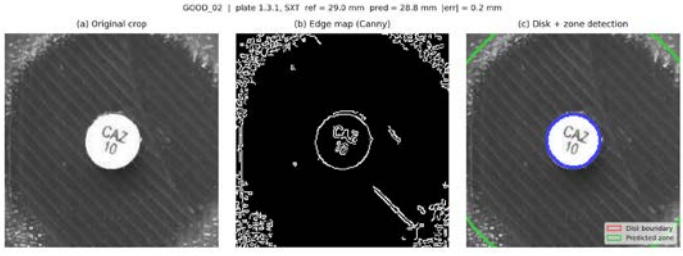


Şekil 5. Bland–Altman grafiği

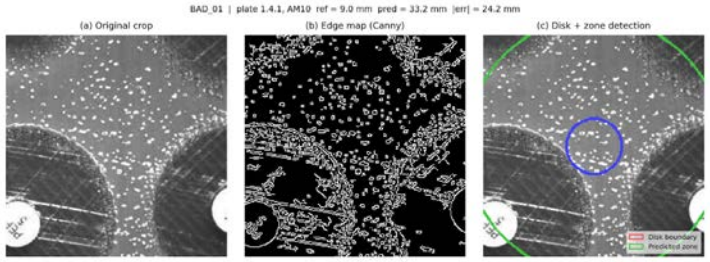
İyi çalışan ve tamamen başarısız birkaç temsilî örnek, orijinal kırpım, kenar haritası ve tespit edilen disk/zon daireleri ile birlikte Şekil 6'da gösterilmiştir.



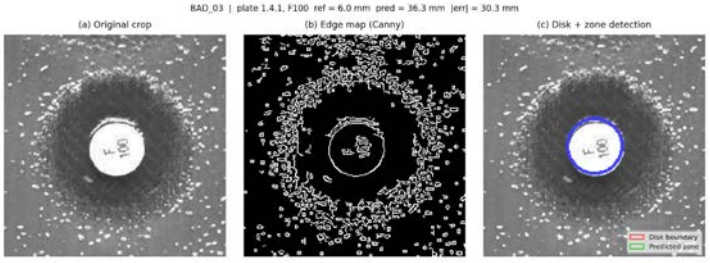
a



b



c



d

Şekil 6. Gradient-CHT yöntemi için örnek disk kesitleri. Her satırda soldan sağa: (a) orijinal yerel plaka kırpımı, (b) Canny kenar haritası, (c) disk sınırı (kırmızı) ve tahmin edilen zon dairesi (yeşil) üst üste bindirilmiş görüntü. Üst satırda düşük hata ile sonuçlanan iki örnek (|err| ≈ 0.1–0.2 mm), alt satırda ise AM10 ve F100 için zon çapının belirgin biçimde olduğundan büyük tahmin edildiği yüksek hatalı örnekler gösterilmektedir.

4. TARTIŞMA

Bu çalışma, disk difüzyon plakalarından inhibisyon zon çaplarının otomatik ölçümü için tamamen açık bir veri kümesi (SIRscan Dryad) üzerinde çalışan, açıklanabilir ve yeniden üretilebilir bir CHT/gradient-tabanlı görüntü işleme hattı sunmaktadır. Elde edilen sayısal sonuçlar, özellikle klinik rutinde beklenen hassasiyet eşiğiyle kıyaslandığında, önerilen yöntemlerin "yüksek doğruluklu otomatik okuma sistemi" olmaktan ziyade, keşif niteliğinde bir temel referans sunduğunu

göstermektedir. Genel düzeyde hem CHT-baseline hem de gradient-CHT yaklaşımı yaklaşık 10 mm mertebesinde ortalama mutlak hata üretmekte; gradient-CHT yöntemi bazı antibiyotik kombinasyonlarında hatayı kısmen azaltırken diğerlerinde benzer ya da daha yüksek hata profilleri ortaya koymaktadır. Bu tablo, klasik dairesel Hough dönüşümü ve türevlerinin, SIRscan veri kümesindeki tüm varyasyonları tek başına yakalamakta zorlandığını, özellikle zon sınırlarının zayıf tanımlandığı veya örtüşen zonların bulunduğu örneklerde yapısal kısıtların belirginleştiğini işaret etmektedir.

Bulgular ayrıntılı incelendiğinde, gradient-CHT'nin yapısal olarak daha tutarlı bir tahmin–referans ilişkisi sunduğu, Pearson korelasyon katsayısının CHT-baseline'a kıyasla belirgin biçimde iyileştiği görülmektedir. Bununla birlikte mutlak hata ölçütleri açısından iki yöntem arasındaki fark sınırlı kalmakta; örneğin AM10, CPD ve F100 gibi belirgin zon sınırlarına sahip antibiyotiklerde gradient-CHT birkaç milimetrelik iyileşme sağlarken, SXT gibi zorlayıcı örüntülere sahip ajanlarda hata düzeyleri yer yer artmaktadır. Bu durum, önerilen gradient-CHT yaklaşımının özellikle kontrastı yüksek, geometrik olarak daha düzenli zonlarda sınır lokalizasyonunu iyileştirebildiğini, ancak zon konturunun bulanıklaştığı, arka plan dokusunun güçlendiği veya komşu zonların birbirine karıştığı senaryolarda gürültüye duyarlı hale geldiğini göstermektedir. Diğer bir ifadeyle, gradyan tabanlı oylama mekanizması yapısal bilginin güçlü olduğu durumlarda avantaj sağlarken, sinyal-gürültü oranının düştüğü örneklerde kararsızlık üretebilmektedir.

Hata desenlerinin antibiyotik bazında farklılaşması, metot performansının yalnızca kullanılan algoritmalara değil, aynı zamanda antibiyotik-bakteri kombinasyonlarının oluşturduğu fenotipik zon morfolojisine de sıkı sıkıya bağlı olduğunu göstermektedir. Örneğin büyük ve keskin kenarlı zonların baskın olduğu CIP gibi ajanlarda her iki yöntem de görece düşük MAE

değerleri üretirken, sınır geçişlerinin daha kademeli olduğu veya koloni adacıklarının zon içinde gözlendiği ajanlarda hata ve bias değerleri artmaktadır. Bu gözlemler, klasik CHT/gradient-CHT yaklaşımının, zonu idealize edilmiş tek bir daire olarak modelleyen varsayımının pek çok gerçek disk difüzyon örneğinde ihlal edildiğini ve bu ihlalin doğrudan ölçüm hatasına yansıdığını ortaya koymaktadır. Aynı zamanda, SIRscan referans ölçümlerinin nasıl üretildiğine ilişkin belirsizlikler (örneğin yarı otomatik veya manuel düzeltme adımları) göz önüne alındığında, "referans" zon çaplarının da belirli bir ölçüde yoruma dayalı olabileceği ve bu nedenle belirli bir taban hata seviyesinin kaçınılmaz olduğu akılda tutulmalıdır. Bu örüntüler, gradient-CHT'nin başarılı ve başarısız olduğu tipik senaryoları gösteren temsilî disk kesitleriyle birlikte Şekil 5'te görsel olarak da izlenebilmektedir.

Çalışmanın bir diğer önemli sonucu, ticari sistemlerin çoğunlukla kapalı kaynaklı yazılım ve tescilli veri kümeleri üzerine kurulu olduğu mevcut ekosistemde, tamamen açık bir veri kümesi üzerinde uçtan uca tanımlanmış bir boru hattının sağladığı şeffaflık ve yeniden üretilebilirlik avantajıdır. SIRscan Dryad veri kümesinin CC0 lisansı altında yayımlanmış olması, bu çalışmada kullanılan plaka seçim kriterlerinin, parametrik yapılandırmaların ve değerlendirme betiklerinin herhangi bir araştırma grubu tarafından aynen tekrarlanmasına imkân tanımaktadır. Bu yönüyle önerilen yöntemler, mutlak hata seviyeleri açısından klinik kullanıma hazır olmasa da, ileride geliştirilecek hem klasik hem de derin öğrenme tabanlı algoritmalar için karşılaştırma yapılabilecek açık bir "benchmark" zemini sunmaktadır. Özellikle antibiyotik bazlı MAE tabloları ve disk seviyesinde sağlanan tahmin–referans çiftleri, farklı algoritmaların belirli ajanlar ve zon morfolojileri üzerindeki güçlü ve zayıf yönlerinin sistematik biçimde karşılaştırılmasına olanak tanımaktadır.

Bu çalışmanın başlıca sınırlılıkları birkaç başlıkta özetlenebilir. Öncelikle analizler, SIRscan Dryad veri kümesinden seçilen yalnızca 20 plaka ve 320 disk ile sınırlıdır; bu nedenle elde edilen hata metriklerinin daha geniş klinik senaryolara genellenebilirliği kısıtlıdır. İkinci olarak, referans zon çapları ticari SIRscan sisteminden alınmış olup, bu ölçümlerin üretiminde olası manuel düzeltme ve operatör etkileri tam olarak bilinememektedir; bu durum, belirli bir taban hata seviyesinin kaçınılmaz olmasına yol açmaktadır. Üçüncü olarak, önerilen yöntemler yalnızca dairesel Hough dönüşümü ve gradyan tabanlı klasik görüntü işleme adımlarına dayanmaktadır; derin öğrenme veya hibrit yaklaşımlar sistematik bir karşılaştırma kapsamında ele alınmamıştır. Mevcut ticari ve araştırma amaçlı otomatik okuyucuların, manuel kumpas ölçümleriyle karşılaştırıldığında çoğu antibiyotik–organizma kombinasyonunda zon çapı farkını birkaç milimetre içinde tuttuğu ve tekrarlı ölçümlerde Sirscan gibi sistemler için zon çapı varyasyonunun genellikle 1–3 mm aralığını aşmadığı bildirilmiştir (Medeiros vd., 2000:1688), (Hombach vd., 2013:1). Bu bağlamda, bu çalışmada raporlanan yaklaşık 10 mm mertebesindeki ortalama mutlak hata, klinik kullanıma hazır otomatik sistemlerde beklenen 1–3 mm düzeyindeki tipik zon çapı sapmalarının belirgin biçimde üzerinde kalmakta ve önerilen yöntemin daha çok açık veri üzerinde keşif amaçlı bir baseline olarak değerlendirilmesi gerektiğini göstermektedir (Medeiros vd., 2000:1688), (Hombach vd., 2013:1), (Costa vd., 2015:104). Son olarak, değerlendirme zon çapı hatası üzerinden yapılmış, antibiyotik duyarlılık kategorilerinin (S/I/R) doğru sınıflandırılması gibi klinik açıdan daha doğrudan çıktılar bu çalışma kapsamının dışında bırakılmıştır.

Tüm bu sınırlılıklara rağmen, çalışma üç açıdan yararlı bir referans noktası sunmaktadır. İlk olarak, tamamen açık lisanslı SIRscan Dryad veri kümesi üzerinde uçtan uca tanımlanmış

CHT/gradient-CHT hattı, disk difüzyon görüntü analizi için kullanılabilir bir benchmark zemini sağlamaktadır. İkinci olarak, antibiyotik bazlı hata profilleri ve iki temel hata modu gibi ayrıntılı hata desenleri, yeni geliştirilecek algoritmalar için somut iyileştirme hedefleri tanımlamaktadır. Üçüncü olarak, parametre ve yapılandırma dosyalarıyla birlikte paylaşılan kod tabanının yeniden üretilebilir olması, bilimsel topluluğa açık, karşılaştırılabilir yöntemler sunma misyonuyla uyumludur.

Gelecek çalışmalar açısından birkaç doğal yönelim ortaya çıkmaktadır. İlk olarak, burada sunulan CHT/gradient-CHT boru hattı, daha gelişmiş kenar/segmentasyon algoritmaları (örneğin seviye kümesi yöntemleri veya graf-tabanlı bölütleme) ile kombine edilerek zon sınırlarının daha esnek geometrik modellerle temsil edilmesi sağlanabilir. İkinci olarak, gradient-CHT'den elde edilen yapısal ipuçlarının, zon konturunu rafine eden hafif derin öğrenme modelleri için ön bilgi olarak kullanıldığı hibrit yaklaşımlar, açıklanabilirlik ile performans arasında daha iyi bir denge sunabilir. Üçüncü olarak, zon çapı hatalarının doğrudan S/I/R kategorilerine yansıması simüle edilerek, ölçüm hatasının klinik karar üzerindeki pratik etkisi nicel olarak değerlendirilebilir; bu sayede "kabul edilebilir hata" aralığı veriye dayalı biçimde tanımlanabilir. Son olarak, farklı laboratuvarlardan ve görüntüleme sistemlerinden elde edilen ek açık veri kümeleriyle yapılacak çok merkezli çalışmalar, hem burada sunulan yöntemlerin genellenebilirliğini sınamak hem de antibiyogram analizi için ortak değerlendirme çerçeveleri geliştirmek açısından kritik olacaktır.

Bu çerçevede, söz konusu çalışma doktora tezinde önerilen gradCHT tabanlı ADT analiz yaklaşımını, güncel bir açık veri kümesi üzerinde yeniden ele alarak nicel performans ve hata desenlerini sistematik biçimde belgeleyen, aynı zamanda gelecekteki yöntemler için açık ve yeniden üretilebilir bir başlangıç noktası sağlayan bir adım olarak değerlendirilebilir.

5. SONUÇ

Bu çalışma, klinik olarak uygulanabilir bir sistem önermeyi amaçlamamaktadır; bunun yerine, açık kaynaklı bir SIRscan veri seti üzerinde şeffaf, tekrarlanabilir bir temel ve ayrıntılı hata analizi sunmayı hedeflemektedir. Disk difüzyon antibiyogram plakalarındaki inhibisyon zonlarının otomatik ölçümü için dairesel Hough dönüşümü ve gradyan tabanlı analiz üzerine kurulu, uçtan uca tanımlanmış ve açık veri kümesi üzerinde çalışan bir görüntü işleme hattı sunmuştur. SIRscan Dryad veri kümesinden seçilen 20 plaka ve 320 antibiyotik diski üzerinde yapılan değerlendirmelerde, hem CHT-baseline hem de gradient-CHT yöntemlerinin yaklaşık 10 mm mertebesinde ortalama mutlak hata ürettiği, gradient-CHT yaklaşımının bazı antibiyotiklerde kısmi iyileşme sağlasa da genel hata seviyesini klinik açıdan yeterli düzeye indiremediği gösterilmiştir. Bu sonuçlar, klasik CHT/gradient-tabanlı yaklaşımların tek başına yüksek doğruluklu otomatik zon okuma sistemi olarak yeterli olmadığını, özellikle düşük kontrastlı ve geometrik olarak karmaşık zon örüntülerinde sistematik hataların devam ettiğini ortaya koymaktadır.

Buna karşın çalışma, tamamen açık lisanslı bir veri kümesi üzerinde parametrik olarak tanımlanmış, kod ve yapılandırma dosyalarıyla yeniden üretilebilir bir temel yöntem ortaya koyarak önem taşımaktadır. Antibiyotik bazlı performans tabloları, disk düzeyinde tahmin–referans çiftleri ve hata desenlerine ilişkin görsel analizler, gelecekte geliştirilecek hem klasik hem de derin öğrenme tabanlı algoritmalar için karşılaştırılabilir bir “benchmark” zemini sunmaktadır. Böylece, kapalı ticari sistemlere dayalı mevcut ekosisteme alternatif olarak, açık veri ve yöntemlerle yürütülen şeffaf antibiyogram analizi çalışmalarına katkı sağlanmaktadır.

Çalışma aynı zamanda yazarın doktora tezinde geliştirilen gradCHT tabanlı ADT analiz yaklaşımının, güncel bir açık veri kümesi ve daha sistematik hata analizi ile yeniden ele alınmış ve genelleştirilmiş hâlini temsil etmektedir. Gelecekte, burada sunulan CHT/gradient-CHT hattının daha esnek segmentasyon teknikleri ve hafif derin öğrenme modelleriyle birleştirilmesi; farklı veri kümeleri ve laboratuvar ortamlarında doğrulanması ve ölçüm hatasının klinik duyarlılık sınıflandırmasına etkisinin nicel olarak incelenmesi, otomatik antibiyogram okuma sistemlerinin doğruluk ve güvenilirliğini artırmaya yönelik temel araştırma başlıkları olarak öne çıkmaktadır.

KAYNAKÇA

Bressan, M., Egli, A., Fiechter, F., Giske, C. G., Hinic, V., Mancini, S., & Nolte, O. (2024). Image dataset of disk diffusion assay scanned with the SIRscan system (Version 1) [Data set]. Dryad. https://doi.org/10.5061/dryad.5dv41nsfj

Costa, L. F., da Silva, E. S., Noronha, V. T., Vaz-Moreira, I., Nunes, O. C., & de Andrade, M. M. (2015). Development of an automatic identification algorithm for antibiogram analysis. Computers in Biology and Medicine, 67, 104–115. https://doi.org/10.1016/j.compbiomed.2015.09.020

Davido, B. (2023). Infections ostéo-articulaires à Entérobactéries multi-résistantes: approche thérapeutique antibiotique optimale (Doctoral dissertation, Université Paris-Saclay).

Dryad Consortium. (2019). Dryad: A data repository for the research community. MIT Libraries. https://libraries.mit.edu/data-management/share/find-repository/dryad/

Evangelista, A. T., & Karlowsky, J. A. (2016). Automated and manual systems for antimicrobial susceptibility testing of bacteria. In Manual of Commercial Methods in Clinical Microbiology: International Edition (pp. 414–432).

Giske, C. G., Bressan, M., Fiechter, F., Hinic, V., Mancini, S., Nolte, O., & Egli, A. (2024). GPT-4-based AI agents—the new expert system for detection of antimicrobial resistance mechanisms? Journal of Clinical Microbiology, 62(11), e00689-24.

Hombach, M., Zbinden, R., & Böttger, E. C. (2013). Standardisation of disk diffusion results for antibiotic susceptibility testing using the SIRscan automated zone

reader. BMC Microbiology, 13, 225. https://doi.org/10.1186/1471-2180-13-225

Jadrná, V. (2025). Detection and measurement of inhibition zones in AST using deep learning. Häme University of Applied Sciences (HAMK)

Joshi, R., Talkute, S., Mane, T., Kushte, S., & Shinde, P. (2022). Disc diffusion antibody sensitivity testing using image processing and machine learning. International Journal of Advanced Research in Science, Communication and Technology, 2(3), 376–380. https://doi.org/10.48175/IJARSCT-3278

Medeiros, M., Crellin, J., & others. (2000). Evaluation of the Sirscan automated zone reader in a clinical microbiology laboratory. Journal of Clinical Microbiology, 38(4), 1688–1693.

Priya, B. K., Reddy, D. A., Rani, A. D., Kalahasthi, N., Soliman, W. G., & Reddy, D. V. R. K. (2023). Automatic inhibition zone diameter measurement for disc diffusion test using image segmentation. IETE Journal of Research, 69(8), 5708–5725. https://doi.org/10.1080/03772063.2021.1953682

Senyer, N., & Efendiyev, C. (2008, April). Automatic antibiogram inhibition zone diameter determination through circular hough transform. In 2008 IEEE 16th Signal Processing, Communication and Applications Conference (pp. 1-4). IEEE.

Uppsala group authors. (2025). Deep learning-based automatic image processing tool to robustly read antibiotic disc diffusion assays: A comprehensive review of image analysis methods for microorganism counting. Uppsala University.

YOLO MİMARİSİ ÜZERİNE BİR DEĞERLENDİRME: TEMEL KAVRAMLAR, ALTYAPI VE KULLANIM ALANLARININ İNCELENMESİ[1]

Kardelen HAS[2]

Durmuş Özkan ŞAHİN[3]

1. GİRİŞ

Çalışmalar Nesne tespiti, bilgisayarlı görü alanında hem akademik araştırmalar hem de endüstriyel uygulamalar açısından temel ve stratejik bir araştırma konusu olarak değerlendirilmektedir. Günümüzde üretim hatlarında otomatik kalite kontrol sistemleri, akıllı şehirlerde trafik izleme ve analiz süreçleri, güvenlik ve gözetim uygulamaları, sağlık alanında görüntü destekli tanı sistemleri ile otonom sürüş senaryoları gibi çok sayıda alanda nesne tespiti, karar destek mekanizmalarının temeli haline gelmiştir. Bu uygulamaların ortak özelliği, sahneden elde edilen görsel verilerin hızlı, güvenilir ve tutarlı biçimde analiz edilmesinin istenmesidir. Dolayısıyla nesne tespit yöntemlerinin yalnızca yüksek doğruluk sunmasının yeterli olmamasına ek olarak; aynı zamanda gerçek zamanlı çalışabilme, düşük gecikme süresi ve donanım kaynaklarını verimli kullanabilme gibi gereksinimlerinin de yerine getirilmesi

---

[1] Ondokuz Mayıs Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği ABD Tezli Yüksek Lisans öğrencisi Kardelen HAS'ın tez çalışması kapsamında bu kitap bölümü oluşturulmuştur.

[2] Yüksek Lisans Öğrencisi, Ondokuz Mayıs Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği ABD, ORCID: 0009-0004-6984-2190.

[3] Dr. Öğr. Üyesi, Ondokuz Mayıs Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, ORCID: 0000-0002-0831-7825.

beklenmektedir (Ali ve Zhang, 2024; Fang vd., 2019; Kang vd., 2025).

Nesne tespiti üzerine yapılan çalışmalarda, geliştirilen yöntemlerin genel olarak çok aşamalı ve tek aşamalı yaklaşımlar etrafında şekillendiği görülmektedir. Çok aşamalı yöntemler, özellikle konumlandırma ve sınıflandırma doğruluğu açısından güçlü sonuçlar üretmekle birlikte, yüksek hesaplama maliyetleri ve uzun işlem süreleri nedeniyle gerçek zamanlı uygulamalarda sınırlı bir kullanılabilirliği vardır. Tek aşamalı yöntemler, hız gereksiniminin ön planda olduğu senaryolarda daha yalın ve pratik çözümlere sahiptir. Bu durum, nesne tespiti problemlerinde hız–doğruluk dengesini gözeten yeni mimari tasarımların geliştirilmesini sağlamıştır (Terven vd., 2023).

Bu gereksinimler doğrultusunda geliştirilen Sadece Bir Kez Bakarsın (You Only Look Once: YOLO) mimarisi, nesne tespit problemini tek bir ağ yapısı ve tek bir ileri besleme adımı içerisinde ele alarak literatürde büyük bir farklılık olmasını sağlamıştır. Sınırlayıcı kutuların ve sınıf olasılıklarının eş zamanlı olarak tahmin edilmesine dayanan bu bütüncül yaklaşım, YOLO'nun hem eğitim hem de çıkarım süreçlerinde yüksek hız sunmasına olanak sağlamıştır. Bu sayede YOLO, özellikle gerçek zamanlı sistemler ve endüstriyel uygulamalar için tercih edilen etkili bir nesne tespit yaklaşımı olmuştur.

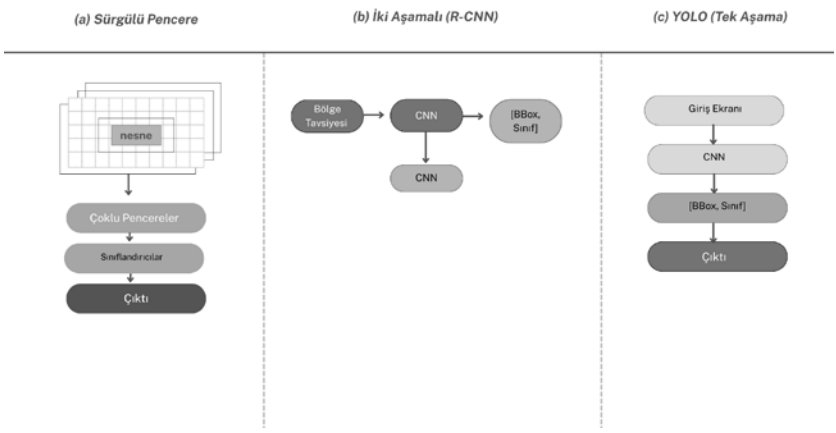
Bu çalışma, YOLO mimarisini temel kavramlar, mimari yapı ve farklı uygulama alanları çerçevesinde ele alarak, yöntemin nesne tespiti literatüründeki konumunu ve pratik uygulamalardaki potansiyelini bütüncül bir bakış açısıyla incelemeyi hedeflemektedir. Bu kapsamda, YOLO'nun geleneksel yaklaşımlara kıyasla sunduğu avantajlar ve farklı kullanım senaryolarındaki rolü detaylı bir şekilde incelenmektedir (Kang vd., 2025).

2. YOLO NEDİR?

YOLO nesne tespiti problemine yönelik geliştirilen tek aşamalı yaklaşımların en bilinen ve en yaygın kullanılan mimarilerden biridir. YOLO mimarisi ilk olarak 2016 yılında Joseph Redmon tarafından tanıtılmıştır. "You Only Look Once" ifadesi, modelin bir görüntüyü yalnızca tek bir geçişte işleyerek nesne tespiti gerçekleştirmesi fikrini yansıtmaktadır (Redmon vd., 2016).

YOLO'nun temel yaklaşımı, nesne tespiti sürecini birbirinden ayrık ve ardışık adımlar halinde yürütmek yerine, problemi tek bir regresyon görevi olarak ele almaya dayanmaktadır. Bu yöntem, modelin bir görüntü üzerinde yalnızca tek bir ileri besleme adımıyla işlem yaptığı vurgulanarak açıklanmaktadır. Ayrıca, tek bir evrişimli sinir ağının birden fazla sınırlayıcı kutu ve bunlara karşılık gelen sınıf olasılıklarını eş zamanlı olarak üretebildiği belirtilmiştir (Ali ve Zhang, 2024). Bu bütüncül yapı, YOLO'nun iki aşamalı yaklaşımlardan ayrılan temel özelliğini açık biçimde ortaya koymakta; nesne tespit sürecinin tek bir ağ üzerinden, tek seferde ve uçtan uca biçimde gerçekleştirilebildiğini göstermektedir (Kang vd., 2025).

Bu yaklaşım sayesinde YOLO mimarisi, yüksek işlem hızlarına çıkabilmekte, gerçek zamanlı uygulamalarda ve donanım kaynaklarında daha etkili şekilde değerlendirebilmektedir. Özellikle gerçek zamanlı sistemler için geliştirilen uygulamalarda, YOLO'nun tek aşamalı mimarisinin sağladığı hız avantajının, kısıtlı hesaplama kaynaklarına sahip ortamlarda dahi nesne tespitini mümkün kıldığı yapılan birçok çalışmada vurgulanmaktadır (Fang vd., 2019).

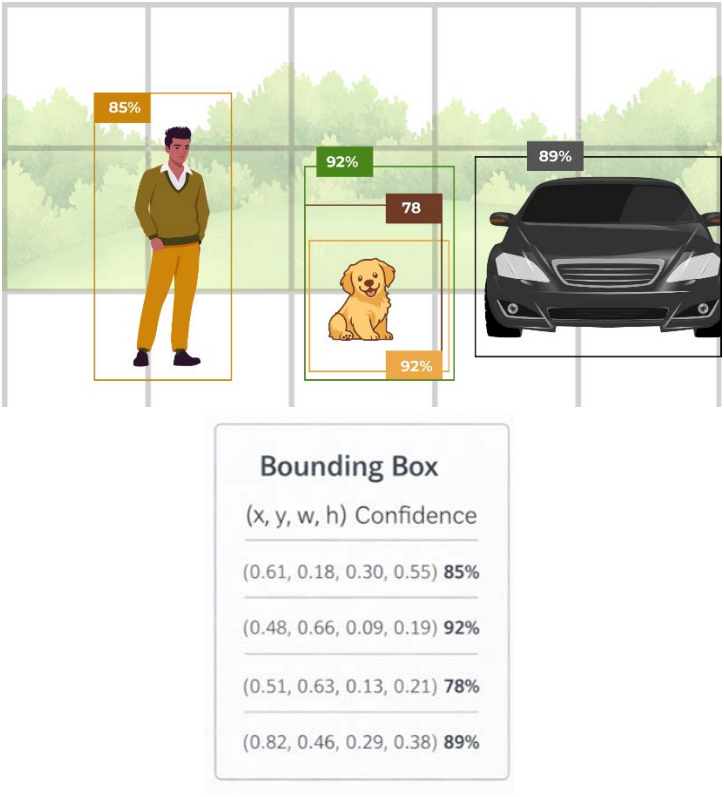


Şekil 1. Kayan pencere tabanlı yöntemler, iki aşamalı (R-CNN) modeller ve tek aşamalı YOLO yaklaşımı arasındaki işlem akışlarının kavramsal karşılaştırması

Bu kapsamda, YOLO yaklaşımının geleneksel kayan pencere tabanlı yöntemler ve iki aşamalı nesne tespit modelleri ile olan kavramsal farkı, Şekil 1'de gösterilmiştir. Ayrıca, tek bir ağ yapısı üzerinden uçtan uca optimizasyon gerçekleştirilebilmesi, eğitim sürecinde kullanılan hedef fonksiyonun doğrudan tespit performansını yansıtacak biçimde şekillenmesine olanak tanımaktadır. Bu yönüyle YOLO, nesne tespiti problemini birbirinden ayrılmış alt bileşenler üzerinden tanımlanan parçalı bir işlem hattı olarak değil, bütüncül ve tekleştirilmiş bir öğrenme problemi olarak ele almaktadır. YOLO'nun sahip olduğu avantajlarının temelinde, mimarinin tek aşamalı bir yapı üzerine tasarlanmış olması yer almaktadır. Bu nedenle izleyen alt bölümde, YOLO'nun temel çalışma prensibi ayrıntılı olarak ele alınmaktadır.

3. YOLO'NUN TEMEL ÇALIŞMA PRENSİBİ

YOLO mimarisinde giriş görüntüsü öncelikle sabit bir boyuta yeniden ölçeklendirilir ve ardından düzenli bir ızgara yapısına ayrılır. Oluşturulan her bir ızgara hücresi, merkez noktası ilgili hücre sınırları içerisinde kalan nesnelerin tespitinden sorumlu olacak şekilde tanımlanır (Ahmad vd., 2020). Bu grid tabanlı tahmin çalışması Şekil 2'de şematik olarak gösterilmektedir.



Şekil 2. YOLO modelinde ızgara tabanlı nesne tespit sürecinin şematik gösterimi

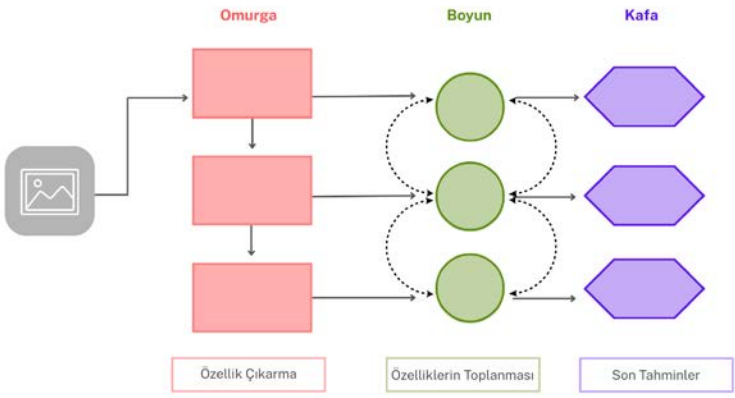
Çalışma, her bir ızgara hücresi için bir veya birden fazla sınırlayıcı kutu, her bir sınırlayıcı kutuya karşılık gelen bir güven skoru ve nesne sınıflarına ait olasılık değerlerini vermektedir. Bu

sonuçlar birlikte değerlendirildiğinde, çalışmada nesnenin varlığına, sınıfına ve konumuna ilişkin bilgileri aynı anda tahmin edebildiği ortaya koymaktadır. Güven skoru, tahmin edilen sınırlayıcı kutunun bir nesne içerme durumunu ve konumsal doğruluğunu birlikte değerlendiren bir değerdir. YOLO mimarisinde bu skor, nesnenin varlığına ilişkin tahmin ile konum uyumunu eş zamanlı dikkate alarak tespit oranını belirlemektedir (Yang vd., 2022). YOLO'nun tek geçişe dayalı ve tek aşamalı yapısı, verinin bütüncül biçimde değerlendirilmesini sağlayarak işlem adımlarını azaltır ve gerçek zamanlı uygulamalarda düşük gecikme ile etkin performans yapısı sağlar. Bu yönüyle YOLO, diğer tek aşamalı nesne tespit yöntemleriyle benzer bir tasarım yapısı sunmaktadır (Fang vd., 2019; Park vd., 2021).

YOLO mimarisinin öne çıkan avantajları, temel olarak hız, mimari sadelik ve bağlam bilgisini etkin kullanabilme yetenekleri sunmaktadır. Tek geçişe dayalı yapısı ile YOLO, video akışları üzerinde yüksek hızlarda çalışabilmekte ve gerçek zamanlı nesne tespiti gerektiren uygulamalar için etkili bir çözüm yolu göstermektedir. Bu özellik, yöntemin ilk kez tanıtıldığı çalışmada da açıkça belirtilmiştir (Redmon vd., 2016). Bunun yanı sıra, tek bir ağ yapısı sayesinde uçtan uca nesne tespiti gerçekleştirebilmesi, YOLO'nun hem eğitim hem de çıkarım süreçlerini sadeleştirmeyi ve kolay uygulamayı sağlamaktadır. Ayrıca görüntüyü bütüncül bir yapı olarak ele alması, karmaşık arka planlara sahip sahnelerde bağlam bilgisinin daha uygun biçimde kullanılmasına fayda sağlamaktadır (Fang vd., 2019). Bu avantajlar sayesinde, YOLO endüstriyel ve gerçek zamanlı uygulamalarda yaygın biçimde kullanılır. Ancak yöntem performansı, uygulama senaryosuna bağlı olarak hız ve doğruluk önceliklerinin dengelenmesini gerektirmekte; veri yapısı, etiketleme kalitesi ve nesne ölçek dağılımı gibi faktörler sistem başarımını büyük ölçüde değiştirmektedir (Kang vd., 2025).

4. YOLO MİMARİSİ ALTYAPISI

YOLO mimarisinin elde ettiği yüksek performans, yalnızca tek aşamalı bir yaklaşım benimsemesinden değil; aynı zamanda derin öğrenme tabanlı mimari bileşenlerin nesne tespiti problemine uygun biçimde tasarlanması ve optimize edilmesinden kaynaklanmaktadır. Güncel YOLO sürümlerinde mimari yapı genel olarak üç temel bileşen altında incelenmektedir. Bunlar Şekil 3'te şematik gösterimi bulunan omurga (backbone), boyun (neck) ve baş (head) yapılarıdır.



Şekil 3. YOLO mimarisinin temel bileşenleri olan backbone–neck–head yapısının şematik gösterimi

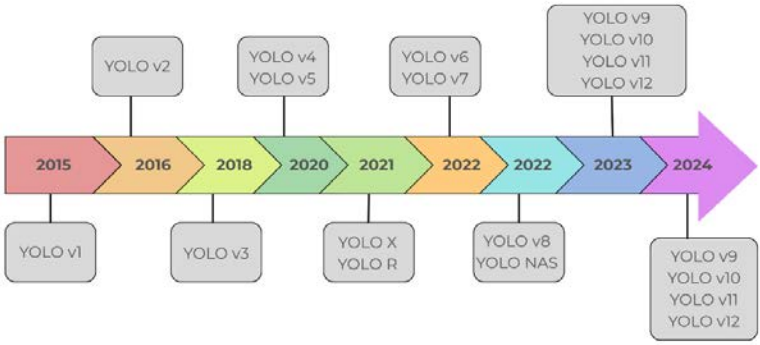
YOLO mimarisi, backbone, neck ve head olmak üzere üç temel bileşen üzerinden uçtan uca bir yapı içerisinde nesne tespiti yapmaktadır. Backbone bileşeni, giriş görüntüsünden ayırt edici ve anlamlı görsel özelliklerin çıkarılmasından sorumlu olup, modelin sahnedeki nesnelere ilişkin temel nesnelerin ortaya çıkarılmasında görev alır. Bu aşamada elde edilen özellikler, hem düşük seviyeli görsel ipuçlarını hem de daha soyut anlamsal bilgileri kapsamaktadır. Neck katmanı, backbone tarafından üretilen bu özellik haritalarını bir araya getirerek çok ölçekli bir temsil yapısı çıkarır. Bu bütünleştirme süreci, özellikle küçük

boyutlu nesnelerin ve karmaşık sahnelerde yer alan hedeflerin daha tutarlı biçimde algılanmasını sağlar. Farklı çözünürlük seviyelerindeki bilgilerin birlikte değerlendirilmesi, modelin sahnenin hem yerel ayrıntılarını hem de küresel bağlamını dikkate alabilmesine fayda sağlar. Head katmanı ise birleştirilen bu özellikler üzerinden nesnelerin konumu, hangi sınıfa ait oldukları ve yapılan tahminlerin güvenilirliğine ilişkin sonuçları verir. Bu aşama, modelin sonuçlarını doğrudan uygulamaya aktarılabilir bir forma dönüştürdüğü son adımı oluşturur.

Bu üç bileşenin tek bir ağ yapısı içerisinde uyumlu ve eş zamanlı biçimde çalışması, YOLO mimarisinin hem yüksek hız hem de dengeli bir doğruluk performansı sunmasına katkıda bulunur. Böylece YOLO, gerçek zamanlı uygulamalarda gerekli olan düşük gecikme gereksinimini karşılarken, farklı ölçek ve karmaşıklıktaki sahnelerde de kararlı bir nesne tespit performansı sunabilir.

4.1. Mevcut YOLO Mimarisi Sürümleri

YOLO mimarisi, ilk versiyonundan itibaren hız–doğruluk dengesini koruyarak performansı artırmayı hedefleyen bir sürece sahiptir. Bu süreçte, modelin temsil gücü çok ölçekli özellik çıkarımıyla güçlendirilirken, gerçek zamanlı çalışma yeteneğinin korunması temel tasarım ilkesi olarak sahiplenilmiştir. YOLO'nun versiyonlar boyunca geçirdiği bu yapısal gelişim, önemli mimari aşamalarla birlikte Şekil 4'te gösterilmektedir.



Şekil 4. YOLO mimarisinin sürümler bazında zaman içindeki gelişiminin kronolojik gösterimi

YOLOv1, tek aşamalı tespit yaklaşımı sayesinde yüksek hız sağlamış; ancak küçük nesnelerin bulunduğu ve sahne yoğunluğunun yüksek olduğu durumlarda belirli sınırlılıklar göstermiştir (Ahmad vd., 2020). YOLOv2 ile birlikte mimari yapı ve eğitim stratejilerinde yapılan iyileştirmeler doğruluk performansını artırmayı hedeflemiştir. YOLOv3, çok ölçekli tahmin yaklaşımını daha belirgin hale getirerek farklı boyutlardaki nesnelerin tespitinde kayda değer iyileşmeler sunmuştur (Kaymakcı vd., 2023). YOLOv4 sürümünde eğitim sürecini destekleyen çeşitli hızlandırıcı teknikler ve mimari optimizasyonlar (örneğin backbone iyileştirmeleri ve veri artırma stratejileri) kullanılarak genel performans yükseltilmiştir. YOLOv5 ve sonrası modeller ise daha modüler bir mimari anlayışı, pratik eğitim süreçleri ve endüstriyel entegrasyon kolaylığı ile öne çıkmış; farklı donanım platformlarına uyarlanabilen ölçeklenebilir model ailesi geliştirme yaklaşımını daha da güçlendirmiştir. YOLO sürümleri arasında yapılan mimari ve yöntemsel farklılıklar, hız, doğruluk ve gerçek zamanlılık gibi temel performans ölçütleri açısından bir gelişim sürecini ifade etmektedir.

5. YOLO MİMARİSİ KULLANIM ALANLARI

YOLO mimarisi, tek aşamalı nesne tespiti yaklaşımı sayesinde gerçek zamanlı uygulamalarda ön planda bulunmaktadır. Tek bir ağ geçişi ile tespit ve sınıflandırmanın birlikte gerçekleştirilmesi, yönteme yüksek hız ve pratiklik sağlamaktadır. Bu özellikleriyle YOLO, farklı uygulama alanlarında yaygın olarak kullanılan bir nesne tespit yaklaşımıdır (Kang vd., 2025). Bu bölümde YOLO mimarisinin farklı alanlardaki kullanımları incelenecektir.

5.1. Gerçek Zamanlı Nesne Tespiti ve Video Analitiği

YOLO mimarisinin en doğal ve yaygın kullanım alanlarından biri, video tabanlı ve gerçek zamanlı algılama gerektiren sistemlerdir. Gerçek zamanlı video analitiği uygulamalarında YOLO mimarisi, özellikle hareketli sahnelerde insan ve araç gibi nesnelerin algılanması, video akışı üzerinde belirli koşullara bağlı olarak olay tetikleme işlemlerinin yapılması (örneğin alarm üretimi, bildirim gönderimi veya kayıt başlatma) ve çoklu nesne takibi yaklaşımlarıyla birlikte kullanılarak nesne sayımı ile izleme görevlerinin yapılması gibi alanlarda sıklıkla tercih edilmektedir (Redmon vd., 2016; Usanmaz ve Güney, 2025).

Bu tür sistemlerde performansı doğrudan etkileyen başlıca faktörler; sahne karmaşıklığı, aydınlatma koşullarındaki değişimler, hareket bulanıklığı, kamera açısındaki farklılıklar ve küçük boyutlu nesnelerin varlığıdır (Peng vd., 2025). YOLO mimarisinin özellikle son sürümlerinde sunulan çok ölçekli tahmin yeteneği, bu zorluklara karşı pratik ve etkili bir çözüm sunarak gerçek zamanlı video analitiği uygulamalarında daha kararlı ve doğru bir algılama sonucu elde edilmesini sağlamıştır (Bochkovskiy vd., 2020; Kang vd., 2025).

5.2. Güvenlik, Gözetim ve Kalabalık Analizi

Güvenlik ve gözetim sistemleri, nesne tespiti yaklaşımlarının en yerleşik ve yaygın kullanım alanlarından biridir. Bu alandaki uygulamalar genellikle insan ve araç tespiti gibi temel görevlerle başlar; zamanla kalabalık yoğunluğu analizi, belirli bölgelerde yığılma tespiti ve yasak alan ihlallerinin belirlenmesi gibi daha üst düzey işlevlere doğru genişler. YOLO mimarisinin bu tür sistemlerde tercih edilmesinin temel nedeni, kamera görüntülerini gerçek zamanlı işleyebilmesi ve buna bağlı olarak hızlı uyarı mekanizmaları üretebilmesidir (Çalışkan ve Demir, 2022).

Kalabalık analizi amacıyla YOLO kullanımının literatürde giderek yaygınlaştığı görülmektedir. Örneğin, kalabalık tespiti ve kişi sayımı problemlerinde YOLOv3 tabanlı yaklaşımların kullanıldığı çalışmalarda, kamera görüntülerinden yaya nesnelerinin tespit edilerek belirli yoğunluk eşiklerine bağlı uyarı sistemlerinin uygulanabilir olduğu gösterilmiştir (Gürevin vd., 2022; Park vd., 2021). Bu tür çalışmalar, YOLO tabanlı çözümlerin özellikle kapasite yönetimi ve kalabalık için erken uyarı senaryolarında pratik bir değer sunduğunu ortaya koymaktadır.

Bu alanda karşılaşılan başlıca zorluklar; sıkışık sahne yapıları, düşük çözünürlüklü veya uzak mesafeden elde edilen yaya görüntüleri ile gece çekimleri, düşük aydınlatma koşulları ve görüntü paraziti gibi olumsuz çevresel etkenler olarak söylenebilir. Bu tür koşullar, özellikle kalabalık alanlarda nesnelerin birbirinden ayırt edilmesini güçleştirmekte ve tespit oranını oldukça kötü oranda etkilemektedir (Zhao vd., 2019; Peng vd., 2025).

Bu zorluklar doğrultusunda literatürdeki güncel araştırma eğilimi, YOLO mimarisinin algılama kapasitesini artırmak amacıyla dikkat mekanizmalarının mimariye dâhil edilmesi ve

daha güçlü çok ölçekli özellik birleştirme yapılarının kullanılması yönünde biçimlenmektedir. Özellikle dikkat tabanlı modüllerin, modelin sahne içerisindeki kritik bölgelere odaklanmasını sağlayarak kalabalık ve karmaşık ortamlarda tespit oranını artırdığı; gelişmiş çok ölçekli özellik birleştirme yaklaşımlarının ise küçük ve örtüşen nesnelerin daha tutarlı biçimde algılanmasına fayda sağladığı farklı çalışmalarda kanıtlanmıştır (Bochkovskiy vd., 2020; Terven vd., 2023).

5.3. Otonom Araçlar, Trafik İzleme ve Akıllı Ulaşım Sistemleri

Otonom sürüş ve akıllı ulaşım sistemlerinde nesne tespiti, güvenli ve kararlı karar üretiminin temel bileşenlerinden biri olarak kabul edilir. Yaya, araç, trafik işaretleri ve levhaları ile şerit üzerindeki engellerin hızlı ve güvenilir biçimde algılanması kritik öneme sahiptir (Li vd., 2025). YOLO tabanlı yaklaşımların kullanıldığı çalışmalarda odak noktası çoğunlukla yaya tespiti ve trafik işareti tanıma gibi güvenlik açısından kritik görevlerdir. Trafik sahnelerinde yaya tespitine odaklanan araştırmalar, YOLO tabanlı modellerin gerçek dünya trafiğinde karşılaşılan karmaşık arka plan yapıları ve küçük hedef problemlerine karşı mimari ve eğitim stratejilerinin belirlenmesinde önemli rol oynadığını göstermektedir. Ayrıca YOLOv3 sürümünün hız–doğruluk dengesine ilişkin raporlanan sonuçları, otonom sürüş gibi gerçek zamanlı sistemlerde YOLO'nun neden yaygın biçimde tercih edildiğini desteklemektedir (Park vd., 2021).

Bu alandaki temel zorluklar; uzak mesafedeki yayalar ve trafik işaretleri gibi küçük boyutlu hedeflerin algılanması, yağmur, sis ve gece sürüşü gibi olumsuz çevresel koşullar ile sahne içeriğinin çok hızlı değişmesi olarak belirtilmektedir. Bu faktörler, algılama sürecinde hem konumsal doğruluğu hem de yakalama oranını olumsuz etkileyerek otonom sürüş sistemlerinin

güvenilirliğinin kapsamını daraltabilmektedir (Ning ve Mi, 2021; Peng vd., 2025).

Bu doğrultuda literatürdeki güncel araştırma eğilimi, YOLO mimarisinde özellikle neck yapısının güçlendirilmesine ve ağın hafifletilerek hız açısından iyileşmesi hedeflenmektedir. Çok ölçekli birleştirme yaklaşımlarının küçük nesnelerin temsillerini güçlendirdiği; hafifletilmiş ağ tasarımlarının ise gerçek zamanlılık gereksinimini korurken yeterli doğruluk seviyelerinin sağlanmasına fayda sağladığı farklı çalışmalarda ifade edilmiştir. Bu yaklaşım, otonom sürüş sistemlerinde doğruluk–hız dengesi açısından daha kararlı ve uygulanabilir çözümler sunmayı amaçlamaktadır (Tan vd., 2020; Bochkovskiy vd., 2020).

5.4. Endüstriyel Uygulamalar, Üretim Hatları ve Kalite Kontrol

Endüstri 4.0 yaklaşımı kapsamında görsel denetim ve otomatik kalite kontrol sistemleri, üretim verimliliği ile süreç güvenilirliği açısından stratejik bir öneme sahiptir (Zhao vd., 2019). YOLO mimarisi bu alanda, üretim süreçlerinin otomatikleştirilmesi ve kalite güvencesinin artırılması amacıyla farklı görevlerde görev almaktadır. Özellikle yüzey kusurlarının tespit edilmesi, eksik parça ya da hatalı montaj durumlarının algılanması ve robotik pick-and-place senaryolarında parçaların konumlarının doğru biçimde belirlenmesi, YOLO tabanlı sistemlerin yaygın olarak tercih edildiği başlıca kullanım alanları arasında bulunmaktadır (Kang vd., 2025).

Yapılan çalışmalarda, özellikle üretim hatlarından elde edilen görüntüler üzerinde YOLO tabanlı modellerin hızlı ve kararlı sonuçlar ortaya koyabildiği ifade edilmiştir (Çalışkan ve Demir, 2022). Özellikle yüzey kusuru denetimi ile tekstil ve fason üretim gibi alanlarda YOLO tabanlı çözümlerin yaygınlaştığı görülmektedir. Örneğin kumaş kusuru tespiti üzerine

gerçekleştirilen kapsamlı çalışmalarda, YOLO ailesinin farklı sürümlerinin kalite kontrol süreçlerinde etkin biçimde kullanılabildiği ve endüstriyel uygulamalar için pratik bir çerçeve sunduğu rapor edilmiştir. Benzer şekilde, metal sac ve levha yüzeylerinde kusur tespitine yönelik YOLO tabanlı modeller öneren çalışmalar da literatürde yer almaktadır (Wang vd., 2023; Ning ve Mi, 2021).

Bu alandaki başlıca zorluklar; kusurların çok küçük ve ince yapıda olması (örneğin çatlaklar ve çizikler), doku karmaşıklığı ve tekrar eden yüzey desenleri ile yanlış pozitif üretimin maliyetinin yüksek olması şeklinde ifade edilebilir. Özellikle hatalı alarmların üretim hattının gereksiz yere durmasına yol açabilmesi, endüstriyel görsel denetim sistemlerinde tespit doğruluğu kadar güvenilirliğin de kritik bir ihtiyaç olduğunu ortaya koymaktadır (Hacıfazlıoğlu ve Aydemir, 2023; Zhao vd., 2019).

5.5. Sağlıkta Görüntü Analizi ve Klinik Karar Destek

Sağlık alanında YOLO, özellikle hızlı tarama gerektiren uygulamalar ve klinik karar destek sistemleri bağlamında önemli bir nesne tespit mimarisidir. Röntgen, bilgisayarlı tomografi ve mikroskop görüntüleri gibi tıbbi görüntüleme verilerinde; lezyon, nodül ve hücresel yapıların tespit edilmesi için çoğu zaman çok sayıda görüntünün kısa süre içerisinde analizinin yapılmış olması gerektirmektedir (Saraei vd., 2025). Bu tür durumlarda, analiz sürecinin yavaşlaması klinik iş akışlarını olumsuz etkilemekle birlikte, tanı süreçlerinde gecikmelere sebep olmaktadır. Bu bağlamda YOLO tabanlı tespitler, gerçek zamanlı veya yarı gerçek zamanlı analiz hedefleyen sistemlerde pratik ve uygulanabilir bir çözüm yolu göstermektedir (Ragab vd., 2024).

Özellikle akciğer röntgenlerinde nodül tespitine yönelik gerçekleştirilen YOLOv3 tabanlı çalışmalar, yöntemin hızlı tarama yöntemlerine daha uygun olduğu ve YOLO mimarisinin

tıbbi görüntü analizi alanına uyarlanabilirliğini kanıtlamıştır. Bu tür çalışmalar, YOLO'nun kısa sürede geniş hasta gruplarına ait görüntüleri analiz edebilmesiyle, radyologlar için ön eleme ve destekleyici bir araç olarak kullanılabileceğini göstermektedir (Karacı, 2022; Redmon vd., 2016).

Daha güncel çalışmalarda ise YOLO tabanlı mimarilerin, yalnızca akciğer nodüllerinin tespitiyle sınırlı kalmayıp; farklı akciğer hastalıkları, tümör oluşumları ve çeşitli lezyon tiplerinin algılanması gibi daha karmaşık durumlarda da doğru raporlar verdiği görülmüştür. Bu çalışmalar, YOLO'nun hız avantajının yanı sıra, uygun veri kümesi ve eğitim stratejileri ile klinik olarak anlamlı sonuçlar verdiğini ortaya koymuştur (Albuquerque vd., 2025). Bununla birlikte, sağlık uygulamalarında hatalı sonuçlar ciddi problemleri beraberinde getirdiği için YOLO tabanlı sistemler çoğunlukla hekim kararlarının yerine geçmekten ziyade, karar destekleyici bir rolü bulunmaktadır. Bu nedenle literatürdeki yaygın yaklaşım, YOLO'nun hızlı ve otomatik tarama kapasitesinden yararlanarak şüpheli bölgelerin önceden işaretlenmesi ve nihai klinik değerlendirmenin uzman hekimler tarafından yapılmasını önermektedir. Bu kullanım biçimi, hem tanı sürecinin hızlandırılmasına hem de klinik iş yükünün azaltılmasına fayda sağlamaktadır (Ragab vd., 2024; Zhao vd., 2019).

5.6. Tarım Teknolojileri ve Çevresel Uygulamalar

Tarım alanında nesne tespiti yaklaşımları; meyve sayımı, verim tahmini, hastalık belirtilerinin belirlenmesi ve hasat otomasyonu gibi pek çok görevde önemli bir rol üstlenir (Kamilaris ve Prenafeta-Boldú, 2018; Santoso vd., 2022). Bu tür senaryolarda YOLO mimarisinin sunduğu hız avantajı, özellikle mobil ve uç cihazlar üzerinde sahada kullanılabilirliği artırmaktadır (Yu vd., 2025).

Örneğin portakal bahçelerinde YOLO tabanlı tespit modelleri kullanılarak meyve algılama ve verim tahmini gerçekleştiren çalışmalarda, transfer öğrenme yaklaşımları sayesinde saha koşullarında uygulanabilir sistemler geliştirilebildiği rapor edilmiştir. Örneğin elma ve narenciye bahçelerinde gerçekleştirilen çalışmalarda, YOLO mimarisinin transfer öğrenme yaklaşımlarıyla saha koşullarına başarıyla benimsendiği ifade edilmiştir (Santoso vd., 2022; Kamilaris ve Prenafeta-Boldú, 2018). Benzer biçimde, armut sayımı amacıyla YOLOv4 ve Deep SORT birlikte kullanılarak geliştirilen bir çalışmada, mobil uygulamalar için gerçek zamanlı sayım sistemlerinin mümkün olduğu ve yüksek ortalama hassasiyet değerlerine ulaşılabildiği gösterilmiştir (Bochkovskiy vd., 2020).

Tarım uygulamalarında karşılaşılan başlıca zorluklar; değişken aydınlatma koşulları, gölge oluşumu ve farklı hava şartları, meyvelerin yaprak ve dallar tarafından kısmen örtülmesi ile benzer renkli arka planların yol açtığı kamuflaj etkisi olarak dikkat çekmektedir. Bu faktörler, özellikle açık alanlarda ve doğal çevre koşullarında yapılan görüntü tabanlı tespit sistemlerinde algılama performansını önemli ölçüde zor bir duruma getirmektedir (Zhao vd., 2019; Kamilaris ve Prenafeta-Boldú, 2018). Bu nedenle veri artırma yöntemleri, farklı gün ve saat koşullarında veri toplanması ve çok ölçekli temsil stratejileri, tarımsal sahalarda YOLO tabanlı sistemlerin performansını belirleyen temel unsurlar arasında yer almaktadır (Tan vd., 2020; Santoso vd., 2022).

5.7. Perakende, Lojistik ve Akıllı Sayım Sistemleri

YOLO mimarisinin yaygınlaştığı bir diğer önemli uygulama alanı perakende ve lojistik sistemleridir. Raf düzeninin kontrolü, ürün sayımı, kasa ve kuyruk analizi ile depo ortamlarında palet ve koli tespiti gibi senaryolarda görüntü tabanlı nesne tespiti çözümlerine ihtiyaç duyulmaktadır. Bu tür

uygulamalarda hız kriteri kritik öneme sahiptir; çünkü kamera akışı süreklidir ve kararların anlık olarak üretilmesi beklenir (Yu vd., 2025). YOLO mimarisinin sunduğu gerçek zamanlı çalışma yeteneği, bu tür dinamik ve yoğun veri akışına sahip ortamlarda bu yöntemin tercih edilmesini sağlayan temel sebeplerdendir.

Perakende ve lojistik ortamlarında gerçekleştirilen YOLO tabanlı çalışmalar, genellikle raf izleme, ürün varlık kontrolü ve otomatik sayım gibi operasyonel süreçlerin iyileştirilmesini sağlamaktadır. Özellikle raf boşluklarının tespiti, yanlış ürün yerleşimlerinin belirlenmesi ve depo içi envanter takibi gibi görevlerde YOLO tabanlı sistemlerin doğru sonuçlar verdiği görülmüştür (Yu vd., 2025). Bununla birlikte mağaza ve depo ortamlarında kamera açıları çoğunlukla sabitlenebildiğinden, veri kümesi oluşturma süreci ve modelin belirli bir ortama uyarlanması görece daha yönetilebilir hale gelmektedir. Bu durum, YOLO tabanlı modellerin kontrollü ortamlarda daha kararlı ve tekrarlanabilir sonuçlar doğurmasını sağlamaktadır (Yu vd., 2025). Bu alanda gerçekleştirilen çalışmaların büyük bölümü uygulama odaklıdır ve genellikle YOLO ailesine ait farklı sürümlerin, hız–doğruluk–model boyutu arasındaki denge dikkate alınarak tercih edildiği görülmektedir (Terven vd., 2023; Kang vd., 2025).

5.8. Robotik Sistemler ve İnsan–Robot Etkileşimi

Robotik uygulamalarda nesne tespiti, robotun çevresini algılaması ve buna bağlı olarak eylem planı oluşturabilmesi için temel girdilerden biridir. Robot kollarının parça alma (pick), yönlendirme ve yerleştirme (place) işlemleri ile insanlarla aynı çalışma alanını paylaşan işbirlikçi robot (cobot) senaryolarında YOLO mimarisinin sunduğu düşük gecikme süresi önemli bir avantaj sağlar (Redmon ve Farhadi, 2017). Endüstriyel ortamlarda robotik sistemler ile YOLO tabanlı algılama modüllerinin birlikte kullanıldığı çalışmalar, algılama–eylem

döngüsünde güvenilirliğin artırılabildiğini ortaya koymaktadır. Özellikle üretim hatlarında parça tanıma, konum doğrulama ve montaj öncesi kontrol gibi görevlerde YOLO tabanlı sistemlerin, robotik kontrol algoritmalarıyla birleştirilerek çevresel farkındalığı artırdığı görülmüştür.

Bununla birlikte robotik uygulamalarda karşılaşılan başlıca zorluklar; nesnelerin farklı yönelimlerde bulunması, kısmi örtülmeler, değişken aydınlatma koşulları ve sahne içerisindeki dinamik hareketler olarak ön plana çıkmaktadır. Bu tür zorluklar, özellikle gerçek zamanlı çalışan robotik sistemlerde algılama performansının sürekliliğini doğrudan değiştirmektedir (Halme vd., 2018). Literatürdeki güncel çalışmalar, bu problemlere yönelik olarak YOLO mimarisinin daha hafif ve hızlı sürümlerinin kullanılması, çok ölçekli temsil yapılarının güçlendirilmesi ve robotik uygulamalara özgü veri kümeleriyle ince ayar yapılması yönünde artış göstermektedir (Terven vd., 2023; Kang vd., 2025). Bu yönüyle YOLO mimarisi, robotik sistemlerde algılama ve karar verme süreçleri arasında etkili bir köprü kurarak, hem endüstriyel robotik hem de insan–robot etkileşimi odaklı uygulamalarda uygulanabilir ve ölçeklenebilir faydalar sağlamaktadır.

6. SONUÇLAR VE DEĞERLENDİRMELER

YOLO mimarisi, nesne tespiti problemini tek aşamalı ve bütüncül bir yaklaşımla ele alarak bilgisayarlı görü alanında önemli bir bakış açısı değişimi sunmuştur (Redmon vd., 2016). Geleneksel çok aşamalı yöntemler yüksek doğruluk potansiyeline sahip olmakla birlikte, hesaplama maliyetleri ve gecikme süreleri nedeniyle gerçek zamanlı uygulamalarda sınırlı bir alana sahip olabilir (Girshick vd., 2014; Ren vd., 2024). YOLO'nun tek bir ağ yapısı üzerinden uçtan uca tahmin üreten tasarım anlayışı, bu sınırlılıkları büyük ölçüde ortadan kaldırarak gerçek zamanlı

nesne tespiti pratik ve uygulanabilir bir duruma getirilmiştir (Redmon ve Farhadi, 2018).

Zaman içerisinde gelişen YOLO sürümleri, temel mimari yaklaşımı korurken temsil gücünü artırmaya ve farklı ölçeklerdeki nesnelerin daha kararlı biçimde sınıflandırılmasını sağlamıştır (Bochkovskiy vd., 2020; Terven vd., 2023). Bu evrim süreci, YOLO'yu yalnızca hızlı bir algılama yöntemi olmaktan çıkararak, hız–doğruluk dengesini gözeten esnek ve ölçeklenebilir bir mimari ailesi durumuna getirmiştir (Kang vd., 2025). Güncel sürümlerde benimsenen modern yapı, farklı donanım platformları ve uygulama senaryoları için uyarlanabilir çözümler sunulmasını sağlamaktadır (Terven vd., 2023).

YOLO mimarisinin birçok alanda kabul görmesinin temel nedenlerinden biri, farklı sektörlerde karşılaşılan gerçek dünya gereksinimlerine etkili biçimde cevaplandırabilmesidir. Endüstriyel üretim ve kalite kontrol süreçlerinden güvenlik ve gözetim sistemlerine, otonom sürüş uygulamalarından sağlık, tarım, perakende ve robotik sistemlere kadar pek çok alanda YOLO tabanlı çözümler, düşük gecikme süresi ve yeterli doğruluk seviyesiyle pratik bir nesne tespit yöntemi halini almıştır (Kang vd., 2025). Bu uygulamaların ortak paydası, algılama sonuçlarının hızlı, kararlı ve sistemlere kolayca entegre edilebilir olması yönündeki çıktılardır (Zhao vd., 2019).

Kullanılan veri kümesinin niteliği, etiketleme sürecinin kalitesi, nesne ölçek dağılımı ve sistemin hız–doğruluk öncelikleri, elde edilen performansı belirleyen temel unsurlar arasında bulunmaktadır (Zhao vd., 2019; Kang vd., 2025). Bu nedenle YOLO, her problem için tek tip bir çözüm olarak değerlendirilmemeli; uygulama gereksinimlerine uygun sürüm, mimari yapı ve eğitim stratejileri bulunarak kullanılmalıdır.

Genel olarak değerlendirildiğinde, YOLO mimarisi nesne tespitinde gerçek zamanlı uygulamaların yaygınlaşmasını

mümkün kılan temel yaklaşımlardan biri olarak sonuç vermektedir (Redmon vd., 2016; Terven vd., 2023). Gelecekte küçük nesne tespiti, yoğun ve karmaşık sahnelerde örtüşen nesnelerin ayrıştırılması, veri verimliliğinin artırılması ve donanım kısıtlarına daha iyi uyum sağlayan hafif mimarilerin geliştirilmesi gibi konuların, YOLO tabanlı sistemlerin çalışma alanını daha da genişletmesi öngörülmektedir (Tan vd., 2020; Kang vd., 2025).

KAYNAKÇA

Ahmad, T., Ma, Y., Yahya, M., Ahmad, B., Nazir, S., & Haq, A. U. (2020). Object detection through modified YOLO neural network. *Scientific Programming*, *2020*(1), 8403262.

Albuquerque, C., Henriques, R., & Castelli, M. (2025). Deep learning-based object detection algorithms in medical imaging: Systematic review. *Heliyon*, *11*(1).

Ali, M. L., & Zhang, Z. (2024). The YOLO framework: A comprehensive review of evolution, applications, and benchmarks in object detection. *Computers*, *13*(12), 336.

Bochkovskiy, A., Wang, C. Y., & Liao, H. Y. M. (2020). Yolov4: Optimal speed and accuracy of object detection. *arXiv preprint arXiv:2004.10934*.

Çalışkan, D., & Demir, Ö. (2022). Derin Öğrenme Yöntemleri ile Şüpheli Davranış Tespiti. *International Periodical of Recent Technologies in Applied Engineering*, *3*(1), 28-43.

Fang, W., Wang, L., & Ren, P. (2019). Tinier-YOLO: A real-time object detection method for constrained environments. *Ieee Access*, *8*, 1935-1944.

Girshick, R., Donahue, J., Darrell, T., & Malik, J. (2014). Rich feature hierarchies for accurate object detection and semantic segmentation. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 580-587).

Gürevin, B., Eğri, S., Gül, R., Gültürk, F., Yıldız, M., & Alquaary, A. (2022). Yolo V4 ile Sahadaki Personelin Yelek Tespiti. *In Doğa ve Mühendislik Bilimlerinde Güncel Tartışmalar 4 (pp. 56-65)*. Bilgin Kültür Sanat Yayınları.

Hacıfazlıoğlu, K., & Aydemir, E. (2023). Görüntü işleme ile kalite kontrol hatalarının tespit edilmesi. *Proceedings of the 2nd International Conference on Innovative Academic Studies*, Konya, Turkey.

Halme, R. J., Lanz, M., Kämäräinen, J., Pieters, R., Latokartano, J., & Hietanen, A. (2018). Review of vision-based safety systems for human-robot collaboration. *Procedia Cirp*, *72*, 111-116.

Kamilaris, A., & Prenafeta-Boldú, F. X. (2018). Deep learning in agriculture: A survey. *Computers and electronics in agriculture*, *147*, 70-90.

Kang, S., Hu, Z., Liu, L., Zhang, K., & Cao, Z. (2025). Object detection YOLO algorithms and their industrial applications: Overview and comparative analysis. *Electronics*, *14*(6), 1104.

Karacı, A. (2022). Detection and classification of shoulder implants from X-ray images: YOLO and pretrained convolution neural network based approach X-isini görüntülerinden omuz implantlarinin tespiti ve siniflandirilmasi: YOLO ve önceden egitilmis evrisimsel sinir agi tabanli bir yaklasim. *Journal of the Faculty of Engineering and Architecture of Gazi University*, *37*(1).

Kaymakcı, Z. E., Akarsu, M., & Öztürk, C. N. (2023, September). Multiple small-scale object detection in aerial vehicle images using standard or optimized yolo detectors. In *2023 International Conference on Innovations in Intelligent Systems and Applications (INISTA)* (pp. 1-5). IEEE.

Li, Y., Zheng, Q., Xu, S., Wang, P., Wang, Y., Song, Z., & Guo, M. (2025). YOLO-EDGE: an object detection algorithm

for traffic scenarios. *The Journal of Supercomputing*, *81*(7), 840.

Ning, Z., & Mi, Z. (2021, May). Research on surface defect detection algorithm of strip steel based on improved YOLOV3. In *Journal of Physics: Conference Series* (Vol. 1907, No. 1, p. 012015). IOP Publishing.

Park, S. S., Tran, V. T., & Lee, D. E. (2021). Application of various yolo models for computer vision-based real-time pothole detection. *Applied Sciences*, *11*(23), 11229.

Peng, E., Ai, Q., Li, Z., Mao, S., & Han, T. (2025). SOG-YOLO: an infrared road scene small object detection model. *The Journal of Supercomputing*, *81*(12), 1209.

Ragab, M. G., Abdulkadir, S. J., Muneer, A., Alqushaibi, A., Sumiea, E. H., Qureshi, R., ... & Alhussian, H. (2024). A comprehensive systematic review of YOLO for medical object detection (2018 to 2023). *IEEE Access*, *12*, 57815-57836.

Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 779-788).

Redmon, J., & Farhadi, A. (2017). YOLO9000: better, faster, stronger. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 7263-7271).

Redmon, J., & Farhadi, A. (2018). *YOLOv3: An Incremental Improvement*. *arXiv preprint arXiv:1804.02767*.

Ren, S., Song, J., Yu, L., & Tian, S. (2024, September). DHC-YOLO: An Improved YOLOv8 for Lesion Detection in Medical Images. In *2024 2nd International Conference on Machine Vision, Image Processing & Imaging Technology (MVIPIT)* (pp. 167-171). IEEE.

Santoso, A. D., Cahyono, F. B., Prahasta, B., Sutrisno, I., & Khumaidi, A. (2022). Development of pcb defect detection system using image processing with yolo cnn method. *International Journal of Artificial Intelligence Research*, 6(1), 343.

Saraei, M., Lalinia, M., & Lee, E. J. (2025). Deep learning-based medical object detection: A survey. *IEEE Access*.

Tan, M., Pang, R., & Le, Q. V. (2020). Efficientdet: Scalable and efficient object detection. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 10781-10790).

Terven, J., Córdova-Esparza, D. M., & Romero-González, J. A. (2023). A comprehensive review of yolo architectures in computer vision: From yolov1 to yolov8 and yolo-nas. *Machine learning and knowledge extraction*, *5*(4), 1680-1716.

Usanmaz, K., & Güney, S. (2025). Derin öğrenme yöntemleriyle trafik işaretlerinin gerçek zamanlı sınıflandırılması. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *40*(2), 1311-1324.

Wang, L., Liu, X., Ma, J., Su, W., & Li, H. (2023). Real-time steel surface defect detection with improved multi-scale YOLO-v5. *Processes*, *11*(5), 1357.

Yang, W., Ding, B. O., & Tong, L. S. (2022, March). TS-YOLO: An efficient YOLO network for multi-scale object detection. In *2022 IEEE 6th information technology and mechatronics engineering conference (ITOEC)* (Vol. 6, pp. 656-660). IEEE.

Yu, H., Fengshou, Z., Gaoshuai, Z., Yuanhao, Q., Aohui, H., & Qingyang, D. (2025). Enhanced YOLOv8 for efficient parcel identification in disordered logistics

environments. *International Journal of Computational Intelligence Systems*, *18*(1), 77.

Zhao, Z. Q., Zheng, P., Xu, S. T., & Wu, X. (2019). Object detection with deep learning: A review. *IEEE transactions on neural networks and learning systems*, *30*(11), 3212-3232.

BİLGİSAYAR BİLİMLERİ VE MÜHENDİSLİĞİ ALANINDA

BİLİMSEL ARAŞTIRMALAR

yaz
yayınları

YAZ Yayınları
M.İhtisas OSB Mah. 4A Cad. No:3/3
İscehisar / AFYONKARAHİSAR
Tel : (0 531) 880 92 99
yazyayinlari@gmail.com • www.yazyayinlari.com