Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi
Niğde Ömer Halisdemir University Journal of Engineering Sciences

Araştırma makalesi / Research article

www.dergipark.org.tr/tr/pub/ngumuh / www.dergipark.org.tr/en/pub/ngumuh

Kötü amaçlı yazılımların transformer modellerle tespiti: Barkod tabanlı görüntüleme ve özellik füzyonu yaklaşımı

Detection of malicious software using transformer models: A barcode-based imaging and feature fusion approach

Zeynep Naz İnan[1, *], Mesut Toğaçar[2]

[1] *Teknoloji ve Bilgi Yönetimi Bölümü, Sosyal Bilimler Enstitüsü, Fırat Üniversitesi,23000 Elazığ, Türkiye*
[2] *Fırat Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri,23000 Elazığ Türkiye*

Öz

Kötü amaçlı yazılımlar, dijital sistemlere zarar verip yetkisiz erişim veya veri hırsızlığına yol açan tehditlerdir. Artan çeşitlilik ve karmaşıklık, klasik tespit yöntemlerini yetersiz bırakmaktadır. Bu çalışmada, zararlı yazılımların tespiti için barkod tabanlı görselleştirme, transformer modeller ile özellik çıkarımı ve makine öğrenmesi sınıflandırmasını birleştiren hibrit bir yaklaşım sunulmaktadır. Çalışmanın ilk aşamasında, 1D formatlı veriler QR ve Aztec barkod türlerine dönüştürülerek 2D veri kümeleri elde edilmiştir. Barkod görüntüleri DeiT3, MaxViT ve Swin Transformer modelleri kullanılarak işlenmiş ve her birinden özellik setleri çıkarılmıştır. Özellik füzyonu adımında, bu setler birleştirilerek zengin bir veri temsili sağlanmıştır. Son aşamada, oluşturulan özellik setleri k-en yakın komşu (kNN) ve destek vektör makinesi (SVM) algoritmaları ile sınıflandırılmıştır. Deneysel analizler, barkod temelli özellik füzyonunun zararlı yazılım tespitinde doğruluğu artırarak %98 başarıya ulaştığını ortaya koymaktadır. Bu çalışma, barkod tabanlı görselleştirme ve transformer temelli füzyonu birleştirerek özgün bir tespit yaklaşımı sunar.

Anahtar kelimeler: Kötü amaçlı yazılım tespiti, transformer modelleri, Barkod tabanlı görselleştirme, Özellik füzyonu, Makine öğrenmesi sınıflandırması

Abstract

Malicious software is a threat that damages digital systems and leads to unauthorized access or data theft. Increasing diversity and complexity render traditional detection methods inadequate. This study presents a hybrid approach combining barcode-based visualization, feature extraction using transformer models, and machine learning classification for detecting malicious software. In the first phase of the study, 1D-formatted data was converted into QR and Aztec barcode types to obtain 2D datasets. The barcode images were processed using DeiT3, MaxViT, and Swin Transformer models, and feature sets were extracted from each. In the feature fusion step, these sets were combined to provide a rich data representation. In the final stage, the created feature sets were classified using K-Nearest Neighbors (kNN) and Support Vector Machine (SVM) algorithms. Experimental analyses indicate that barcode-based feature fusion enhances malware detection accuracy, achieving a 98% success rate. This study presents a novel detection approach by combining barcode-based visualization and transformer-based fusion.

Keywords: Malware detection, Transformer models, Barcode-based Visualization, Feature fusion, Machine learning classification

1 Giriş

Günümüzde dijital teknolojilerin yaşamın her alanına entegre olmasıyla birlikte, bilgi sistemlerini hedef alan kötü amaçlı yazılımlar, siber güvenlik açısından en ciddi tehditlerden biri haline gelmiştir. Sistemlere zarar vermek, hassas verileri ele geçirmek veya yetkisiz erişim sağlamak amacıyla geliştirilen bu yazılımlar, gelişen teknolojilerle birlikte daha karmaşık yapılara bürünmektedir. Günümüzde yalnızca bir gün içinde tespit edilen yeni zararlı yazılım sayısının 500 bini aştığı ve toplamda bilinen zararlı yazılım örneklerinin 1 milyarın üzerinde olduğu bildirilmektedir [1]. Artan tehdit çeşitliliği, mevcut imza temelli ve davranışsal analiz yaklaşımlarının sınırlılıklarını gözler önüne sermiş ve daha yaratıcı güvenlik çözümlerine olan ihtiyacı derinleştirmiştir.

Bu doğrultuda, yapay zekâ ve makine öğrenmesi tabanlı yöntemlerin kötü amaçlı yazılım tespitinde kullanılmasına yönelik araştırmalar artış göstermiştir. Muhati ve Rawat, ağ trafiği üzerinde gerçekleşen anomalilerin veri odaklı görselleştirme yöntemleriyle analiz edilmesini sağlamış ve siber saldırıların daha iyi anlaşılması için etkili bir yaklaşım ortaya koymuştur [2]. Ullah ve arkadaşları ise metin ve görsel verileri bir arada işleyerek transformer tabanlı transfer öğrenme yaklaşımıyla açıklanabilir bir kötü amaçlı yazılım tespit sistemi geliştirmiştir [3]. Alqahtani ve çalışma arkadaşları, derin öğrenme temelli bir boyutlu evrişimli sinir ağı (1D-CNN) modeli kullanarak çalıştırılabilir dosyaların statik başlık bilgileri üzerinden zararlı yazılım tespitinde yüksek doğruluk sağlamışlardır [4]. Ashawa ve arkadaşları tarafından geliştirilen çalışmada ise, CNN ve transformer mimarileri birleştirilerek görsel

* Sorumlu yazar / Corresponding author, e-posta / e-mail: zeynep.nazelazig@gmail.com (Z. N. İnan)
Geliş / Received: 27.10.2025 Kabul / Accepted: 20.01.2026 Yayımlanma / Published: 30.01.2026
doi: 10.28948/ngumuh.1811827

tabanlı zararlı yazılım sınıflandırmasında ünlü performans elde edilmiştir [5]. Xue ve arkadaşları, birden fazla kod kanalını içeren çok kanallı bir kod görselleştirme yöntemi kullanarak zararlı yazılımların tespitine katkı sağlamışlardır [6]. Hafeth ve Abdullahi tarafından sunulan HRT-Net yöntemi ise ResNet ve Transformer mimarilerini bir araya getirerek özellik seçimi için İyileştirilmiş çekirge optimizasyon algoritması (IGOA) entegre etmiş ve çeşitli zararlı yazılım verileri üzerinde başarılı sınıflandırma sonuçları elde etmiştir [7]. Ayrıca, Qian ve arkadaşlarının CAFTrans modeli, API çağrı dizilerindeki kanal özelliklerini ve API frekansı bilgilerini dikkate alan özel bir transformer tabanlı model sunarak kötü amaçlı yazılımların daha etkili şekilde tespit edilmesini sağlamıştır [8].

Mevcut çalışmalarda görselleştirme temelli analizler yer alsa da barkod tabanlı veri görselleştirme yöntemleriyle zararlı yazılım tespiti konusunda literatürde sınırlı çalışma bulunmaktadır. Barkodlar; kompakt veri temsili, yüksek bilgi yoğunluğu ve hata düzeltme yetenekleriyle bu alanda alternatif bir çözüm sunmaktadır. Bu çalışmada, kötü amaçlı yazılımların tespitinde barkod tabanlı görselleştirme ile transformer destekli özellik çıkarımını birleştiren hibrit bir model önerilmiştir. Bu hibrit model, barkod temelli veri görselleştirme yöntemini transformer modellerin güçlü temsil kapasitesiyle bir araya getirerek kötü amaçlı yazılım tespitinde yüksek doğruluk sağlamayı amaçlamaktadır.

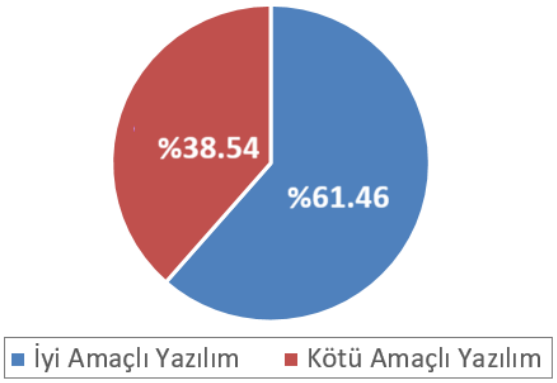
Bu çalışmanın amacı ve hedefleri şu şekilde özetlenebilir:

- Kötü amaçlı yazılımların tespitinde, geleneksel yöntemlerin ötesine geçerek yenilikçi ve görsel bir analiz yaklaşımı sunmak,
- Metin tabanlı kötü amaçlı yazılım verilerini, daha verimli özellik çıkarımı sağlamak amacıyla barkod türlerine dönüştürmek ve bu verileri iki boyutlu (2B) transformer modelleri ile eğitmek,
- Elde edilen barkod tabanlı görsel veriler üzerinden yeni nesil transformer modelleri ile öznitelik çıkarmak,
- Çıkarılan öznitelikleri, özellik füzyonu yöntemiyle birleştirerek daha zengin bir temsil oluşturmak,
- Oluşturulan özellik vektörlerini makine öğrenmesi algoritmalarıyla sınıflandırmak ve performanslarını karşılaştırmak.

2 Veri kümesi

Somlap, Hindistan Centurion Teknoloji ve Yönetim Üniversitesi araştırmacıları tarafından windows tabanlı exe dosyası olarak oluşturulmuş ve kötü amaçlı yazılım verilerini içeren açık erişimli bir veri kümesidir. Somlap verileri, hem iyi huylu hem de kötü amaçlı yazılım içeren 51.409 örnekten oluşmaktadır. Veriler, Virus Share'den toplanan 19.809 kötü amaçlı yazılım dosyası özelliği ve Windows 10 işletim sisteminden toplanan 31.600 iyi huylu yürütülebilir dosya ve DLL içermektedir [9]. Veri kümesinin yüzdelik oranı Şekil 1'de ifade edilmiştir.

Bu veri kümesi 109 sütundan oluşmuştur. Son sütunda yer alan "class" hedef değişken olarak kullanılmıştır [10]. Somlap veri kümesindeki veriler 2B barkod formatlarına çevrilmiştir. Barkod görselleştirme işlemi sırasında, verilerin karakteristik yapısı korunarak hem insan hem de model odaklı analizleri kolaylaştıracak bir görsel yapı elde edilmesi hedeflenmiştir. Bu kapsamda, her bir veri örneği QR ve Aztec barkod türleri kullanılarak iki farklı görsel forma dönüştürülmüştür.



Şekil 1. Veri kümesinin türleri ve yüzdelik oranları

Veri kümesinde yer alan yüksek sayıda örneğin işlenmesi ve eğitim süresinin verimliliği açısından, her barkod türü için ilgili sınıfa ait tüm örnekler arasından eşit sayıda (1000 adet) örnek, yazılım tarafından otomatik olarak rastgele seçilerek analiz süreci yürütülmüştür. Bu süreçte her sınıf kendi içinde ayrı ayrı örneklenmiş, böylece rastgelelik korunurken sınıflar arası örnek sayısı dengesi de sağlanmıştır. İnsan müdahalesi olmaksızın gerçekleştirilen bu seçim süreci, çalışmada sınıf dengeli kontrollü rastgele örnekleme yöntemi olarak incelenmiştir. Seçilen örnekler, derin özellik çıkarımı ve sınıflandırma adımlarında model eğitim sürecinde kullanılmıştır.

3 Yöntem ve yaklaşımlar

3.1 Aztec ve QR teknikleri

Aztec barkodları, kompakt yapıları ve veri yoğunluğu sağlama potansiyelleri nedeniyle iki boyutlu barkod teknolojileri arasında dikkat çekmektedir. Bu barkod türü, merkezde yer alan hedef deseni sayesinde dış kenar boşluklarına ihtiyaç duymadan tanımlanabilmekte ve verinin merkezden dışa doğru yerleştirilmesi tarama sürecini kolaylaştırmaktadır. Bu yapısal özellikler, Aztec barkodların çeşitli uygulama senaryolarında tercih edilmesine olanak sağlamaktadır [11].

QR (Quick Response) kodları, 2B barkod sistemleri arasında geniş veri kapasitesi ve güçlü hata düzeltme mekanizması sayesinde ön plana çıkan etkili bir görselleştirme tekniğidir. Dış çevresel bozulmalara karşı dayanıklılığı, Reed–Solomon algoritması ile sağlanan hata toleransı ile desteklenmektedir. Bu sayede, veri alanının belirli bölümleri zarar görse bile kodun genel yapısı bozulmadan korunabilir. Bu özellik, özellikle düşük çözünürlüklü ortamlarda bile güvenilir veri okuma imkânı sunmaktadır. Yi ve arkadaşlarının gerçekleştirdiği çalışmada, QR kodlarının bozulmuş ve düşük kaliteli görseller üzerinde dahi yüksek doğrulukla çözümlenebildiği

ve gelişmiş görsel düzeltme teknikleriyle başarıyla yeniden yapılandırılabildiği gösterilmiştir [12].

Bu bağlamda, çalışma kapsamında metin tabanlı kötü amaçlı yazılım örnekleri QR ve Aztec barkod biçimine dönüştürülerek bilgi içeriği yüksek, kompakt ve analiz odaklı görsel yapılar elde edilmiştir. Bu dönüştürme süreci, sınırlı alanlarda veri yoğunluğunu artırmayı hedeflemiş ve makine öğrenmesi algoritmaları tarafından daha verimli kullanılabilecek örnekler oluşturulmasını sağlamıştır. Elde edilen bu barkodlar, sonraki adımlarda kullanılmak üzere özellik çıkarımı ve sınıflandırma süreçlerinde girdi olarak değerlendirilmiştir.

3.2 Transformer modeller

Transformer mimarisine dayalı modeller, görüntü işleme alanında sundukları yüksek performans ile geleneksel yaklaşımlara kıyasla önemli avantajlar sağlamaktadır. Bu çalışmada, barkod görselleştirmesi ile elde edilen verilerden anlamlı ve derinlemesine özellik çıkarımı gerçekleştirmek amacıyla üç güncel transformer modeli tercih edilmiştir: DeiT3, MaxViT ve Swin. Aşağıda, her bir modelin mimari yapısı ve çalışma prensiplerine ilişkin özet bilgiler sunulmuştur.

DeiT (Data-efficient Image Transformer) modeli, görüntü sınıflandırma alanında az veriyle yüksek doğruluk elde edilmesi amacıyla ortaya konmuş gelişmiş bir görsel dönüştürücü modelin türevidir. Bu sürüm, ViT tabanlı mimarinin üçüncü versiyonu olup, dikkat mekanizmasını iyileştiren ve eğitim sürecinde distilasyon tekniklerini kullanan bir yapıya sahiptir. Literatürde, DeiT tabanlı mimarilerin hem küçük ölçekli hem de daha geniş veri kümelerinde istikrarlı ve güvenilir sonuçlar verdiği ifade edilmiştir [13]. Bu çalışmada geliştirilen üçüncü sürüm olan DeiT3 tercih edilmesinin sebebi daha derin yapılarla, iyileştirilmiş eğitim teknikleriyle ve farklı düzenleme yöntemleriyle daha kararlı ve daha yüksek doğruluk sağlamayı hedeflemiştir. DeiT3 barkod formatına dönüştürülen zararlı yazılım verilerindeki bilgi yoğun desenleri analiz etmek için tercih edilmiştir. Modelin öne çıkan yönü, sınırlı veri miktarında dahi etkili öznitelikler çıkarabilmesi ve bu özniteliklerin sonraki sınıflandırma aşamalarında doğruluğu artıracak bir temel oluşturmasıdır.

MaxViT (Maximized Vision Transformer) modeli, aynı anda hem yerel hem de küresel bilgilerin öğrenilmesine imkân tanıyan çok eksenli bir vizyon dönüştürücü mimarisi olarak geliştirilmiştir. Modelde pencere tabanlı dikkat mekanizması ile ızgara tabanlı küresel dikkat katmanları bir araya getirilmiş ve çok ölçekli görsel temsillerin elde edilmesi sağlanmıştır. Bu yaklaşım, farklı çözünürlüklerdeki bilgilerin bütünleşik bir şekilde değerlendirilmesine olanak tanımıştır [14]. Çalışmada MaxViT, barkod görsellerinde hem küçük ölçekli ayrıntıların hem de genel yapısal desenlerin yakalanabilmesi amacıyla kullanılmıştır. Bu sayede, elde edilen özniteliklerin çeşitliliği artmış ve sınıflandırma sürecinde daha dengeli bir temsil oluşturulmuştur.

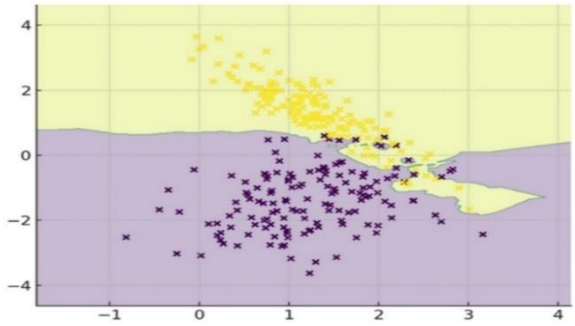
Swin Transformer modeli, hiyerarşik yapısı ve kaydırmalı pencere mekanizmasıyla farklı çözünürlük seviyelerinden bilgi çıkarabilen bir mimari olarak geliştirilmiştir. Görüntüler küçük parçalara ayrılarak işlenmekte, ardından pencere kaydırmaları sayesinde daha geniş bağlamlar öğrenilmektedir. Bu yöntem sayesinde hem yerel ayrıntılar hem de genel yapısal ilişkiler aynı anda yakalanabilmektedir. Çeşitli araştırmalarda, bu mimarinin çok ölçekli görsel veriler üzerinde yüksek doğruluk sunduğu ve işlem verimliliğini koruduğu ortaya konmuştur [15]. Çalışmada Swin Transformer, QR ve Aztec barkod görsellerinden zengin öznitelikler elde edilmesi için kullanılmıştır. Modelin çok ölçekli temsil üretme özelliği sayesinde, sınıflandırma sürecine daha kapsamlı ve dengeli bir katkı sağlanmıştır.

3.3 Makine öğrenme yöntemleri

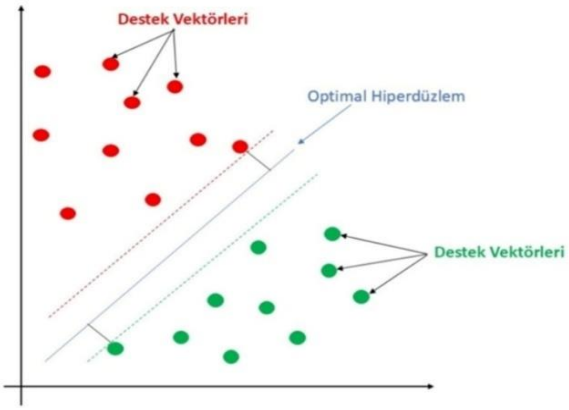
Makine öğrenmesi, verilerden öğrenilen istatistiksel ilişkiler aracılığıyla tahmin veya sınıflandırma yapılmasını sağlayan bir yöntemler bütünüdür. Geleneksel programlama anlayışında karar kuralları doğrudan geliştirici tarafından belirlenirken, makine öğrenmesi yaklaşımlarında bu kurallar verilerin kendisinden çıkarılmaktadır. Böylece, sistemler yeni örnekler karşısında otomatik olarak uyum sağlayabilmektedir. Özellikle sınıflandırma problemlerinde makine öğrenmesi algoritmaları, farklı sınıfları ayıran sınırların istatistiksel ve geometrik temsiller üzerinden belirlenmesine olanak tanımaktadır. Bu bağlamda, bazı yöntemler basit mesafe ölçütlerine dayalı karar mekanizmaları kurarken, bazıları ise karmaşık fonksiyonlar aracılığıyla daha esnek sınırlar çizmektedir [16]. Çalışmada, barkod tabanlı görsellerden elde edilen özniteliklerin ayrıştırılmasında güçlü ve yaygın biçimde kullanılan iki yöntem olan k-En Yakın Komşu (kNN) ve Destek Vektör Makineleri (SVM) tercih edilmiştir. kNN algoritması, örnekler arasındaki mesafe ölçütlerine dayanarak sınıflandırma yapan basit fakat etkili bir yöntemdir. Yeni bir örneğin sınıfı, eğitim kümesindeki en yakın komşularının çoğunluğuna göre belirlenmektedir. Mesafe ölçümünde genellikle Öklid veya Manhattan metriği kullanılmaktadır. Algoritmanın anlaşılır yapısı, küçük ölçekli veri kümelerinde yüksek doğruluk sağlamasına imkân tanımaktadır; ancak büyük boyutlu verilerde hesaplama maliyetinin artması bir sınırlılık olarak değerlendirilmektedir. Yapılan araştırmalarda, kNN yönteminin kötü amaçlı yazılım tespitinde özellikle izin tabanlı özelliklerin analiziyle güçlü sonuçlar verdiği rapor edilmiştir [17]. Bu çalışmada kNN, barkod görsellerinden çıkarılan özniteliklerin sınıflandırılmasında temel yöntemlerden biri olarak uygulanmıştır. kNN algoritmasının sınıflandırma sürecinde örneklerin karar bölgelerine göre dağılımı Şekil 2'de gösterilmektedir.

SVM, farklı sınıfları ayırmak için en uygun hiper düzlemin bulunmasına dayalı bir sınıflandırma yöntemidir. Bu yaklaşımda, sınıflar arasındaki marjin en üst düzeye çıkarılmakta ve böylece genelleme başarısı artırılmaktadır. Doğrusal olmayan verilerde çekirdek fonksiyonları kullanılarak daha esnek karar sınırları elde edilmektedir. Yöntemin özellikle yüksek boyutlu veri kümelerinde güçlü bir performans gösterdiği çeşitli çalışmalarda ortaya konmuştur [18]. Bu kapsamda, SVM barkod tabanlı özniteliklerin sınıflandırılmasında kullanılmış ve elde

edilen temsillerin daha yüksek doğruluk oranlarıyla ayrıştırılmasına katkı sağlamıştır. SVM algoritmasında sınıflar arasındaki ayrımı sağlayan optimal hiper düzlem ve destek vektörlerinin örnek gösterimi Şekil 3'te gösterilmektedir.



Şekil 2. kNN algoritmasının sınıflandırma sürecinde gerçekleştirilmiş örnek gösterimi

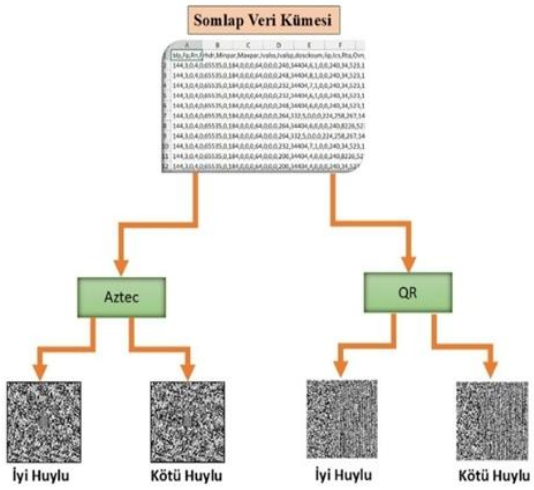


Şekil 3. SVM algoritmasında hiper düzlemin ve destek vektörlerinin örnek gösterimi

3.4 Önerilen yaklaşım

Önerilen yaklaşımın ilk aşamasında Somlap veri kümesi kullanılmıştır. Bu kümede hem iyi huylu hem de kötü amaçlı yazılım örnekleri yer almakta olup, özellikle Windows tabanlı yürütülebilir dosyalardan elde edilmiş çeşitli nitelikler barındırmaktadır. Çalışmada, bu kümenin bütünlüğü korunmuş ancak sınıflandırmaya yönelik olarak hedef değişken olarak belirlenen "class" sütunu kullanılmıştır. Veri kümesindeki "class" sınıfı barkod dönüşümlerde dahil edilmemiştir. Veri kümesindeki diğer niteliklerde ise bazı sürekli değişen değerler için belirli bir eşik değer aralığı oluşturulmuş ve bu eşik değerleri kategorik olarak sınıflandırılmıştır. Böylece, her bir örneğin kötü amaçlı veya iyi huylu olarak tanımlanması sağlanmış ve sonraki adımlar için temel oluşturulmuştur.

İkinci adımda, metin tabanlı yazılım verileri iki boyutlu görsel yapılara dönüştürülmüştür. Bunun için QR ve Aztec barkod türleri tercih edilmiştir. Bu barkodlar, yüksek bilgi yoğunluğu ve hata düzeltme yetenekleri sayesinde verilerin görsel forma taşınmasını sağlamaktadır. Dönüşüm işlemi sırasında verilerin özgün yapısı korunmuş, böylece model tabanlı analiz için uygun bir temsil elde edilmiştir. Bu işlem sonucunda her bir yazılım örneği için iki farklı barkod görseli oluşturulmuştur. 1B veri kümesinin Aztec ve QR olmak üzere iki farklı 2B barkod türüne dönüştürülme süreci Şekil 4'te gösterilmektedir.



Şekil 4. 1B veri kümesinin 2B barkod türlerine dönüştürülmesi işlemi

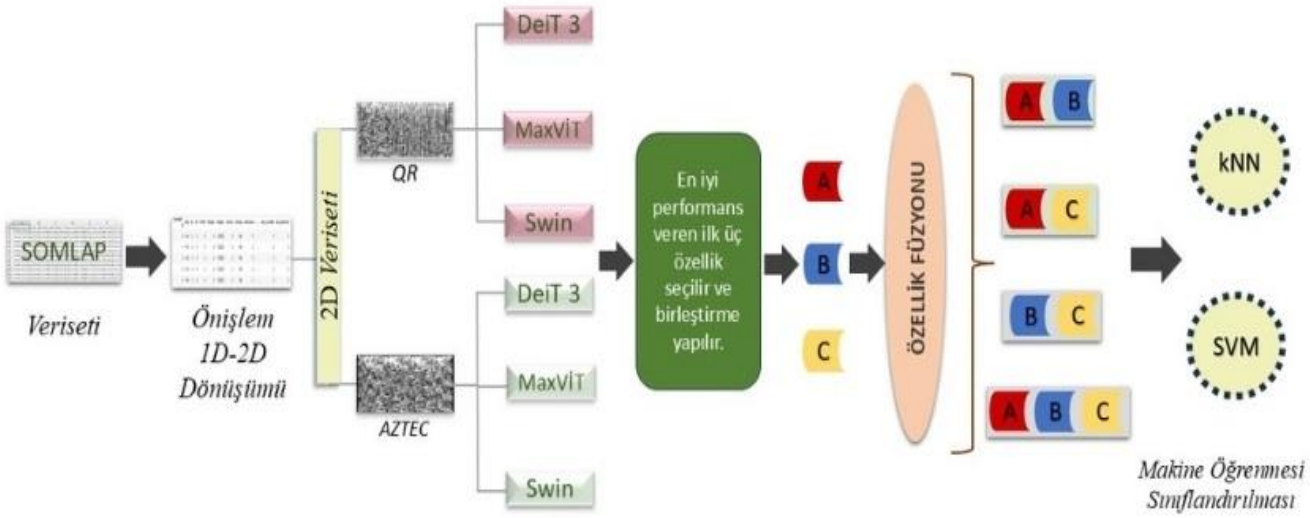
Veri kümesinin büyüklüğü nedeniyle tüm örneklerin işlenmesi yerine her barkod türü için rastgele 1000 örnek seçilmiştir. Böylece hem işlem süresi optimize edilmiş hem de eğitim aşamasında dengeli bir örneklem kullanılmıştır. Seçilen bu örnekler, sonraki aşamalarda öznitelik çıkarımı için girdi olarak kullanılmıştır.

Elde edilen barkod görsellerinden anlamlı özellikler çıkarılabilmesi için üç farklı transformer tabanlı modelden yararlanılmıştır: DeiT3, MaxViT ve Swin Transformer. Bu modeller, görsel veriler üzerinde çok katmanlı dikkat mekanizmaları kullanarak, barkodlardaki ince desenleri ve yapısal ilişkileri yakalamada etkinlik göstermektedir. Böylece her barkod için yüksek boyutlu ve ayırt edici öznitelik setleri oluşturulmuştur.

Transformer modellerinden elde edilen öznitelikler daha güçlü bir temsil sağlamak amacıyla özellik füzyonu tekniğiyle birleştirilmiştir. Bu aşamada, farklı barkod türlerinden ve modellerden elde edilen öznitelikler ortak bir yapıya entegre edilerek daha zengin ve çeşitlendirilmiş bir veri kümesi oluşturulmuştur. Böylece, tek bir kaynaktan elde edilen özniteliklerin sınırlılıkları azaltılmış ve sınıflandırma performansının artırılması hedeflenmiştir.

Son aşamada, oluşturulan öznitelik seti makine öğrenmesi algoritmalarına aktarılmıştır. Bu kapsamda, kNN ve SVM kullanılarak kötü amaçlı yazılımların sınıflandırılması gerçekleştirilmiştir. kNN algoritması örnekler arası benzerlik üzerinden tahmin yaparken, SVM en geniş marjinli sınır çizgisi ile farklı sınıfları ayırmıştır.

Bu çalışmada, önişlem basamakları ile kullanılan transformer modeli Python programlama dili kullanılarak kodlanmış ve analizler Google Colab ortamında gerçekleştirilmiştir. Çalışmada önerilen yöntemin genel mimarisi ve işlem akışı Şekil 5'te gösterilmektedir.



Şekil 5. Önerilen yaklaşımın genel tasarımı

Kodların derlenmesi için Jupyter Notebook platformundan yararlanılmıştır. Sınıflandırma sürecinde MATLAB programı kullanılmıştır. Analizlerin değerlendirilmesinde karmaşıklık matrisi (confusion matrix) tercih edilmiştir. Karmaşıklık matrisi, tüm örneklerin eşit şekilde hesaba katıldığı mikro ortalamalı doğruluk yöntemi kullanılarak hesaplanmıştır. Bu yapı sayesinde sınıflandırma algoritmalarının hangi hataları ürettiği ve bu hataların dağılımı sistematik bir şekilde analiz edilebilmiştir [19]. Bu matrisin hesaplanmasında kullanılan performans ölçütleri; geri çağırma, kesinlik, F-skoru ve doğruluk değerleridir [20]. Denklem (1) ve Denklem (4) arasında ifade edilen kısaltmalar belirli anlamlara sahiptir. Buna göre sınıflardan biri pozitif (P), diğeri ise negatif (N) olarak etiketlenmiştir. Çok sınıflı sınıflandırma problemlerinde karmaşıklık matrisi N×N boyutunda tanımlanır ve burada N, sınıf sayısını ifade eder. Bu tür problemlerde doğru pozitif (DP), yanlış pozitif (YP), doğru negatif (DN) ve yanlış negatif (YN) kavramları doğrudan kullanılamaz; bunun yerine her bir sınıf tek tek ele alınır. İncelenen sınıf pozitif kabul edilirken, geri kalan tüm sınıflar negatif olarak değerlendirilir [21, 22]. Önerilen yaklaşımda kullanılan model ve yöntemlerin parametre bilgileri Tablo 1'de verilmiştir.

$$\text{Geri çağırma} = \frac{DP}{DP+YN} \quad (1)$$

$$\text{Kesinlik} = \frac{DP}{DP+YP} \quad (2)$$

$$\text{F-skor} = \frac{2\times\text{Kesinlik}\times\text{Duyarlılık}}{\text{Kesinlik}+\text{Duyarlılık}} \quad (3)$$

$$\text{Doğruluk} = \frac{DP+DN}{YP+YN+DP+DN} \quad (4)$$

Ayrıca önerilen yaklaşımın sınıflandırma aşamasında kullanılan makine öğrenmesi yöntemlerinin parametreleri, "MATLAB-Classification Learner" ortamında gerçekleştirilen ön değerlendirme denemeleri sonucunda belirlenmiştir. Bu kapsamda, SVM için linear, quadratic, cubic ve gaussian çekirdek fonksiyonları; kNN için ise farklı komşuluk ve uzaklık metrikleri denenmiş ve en yüksek doğruluk değerini sağlayan seçimler nihai deneylerde kullanılmıştır.

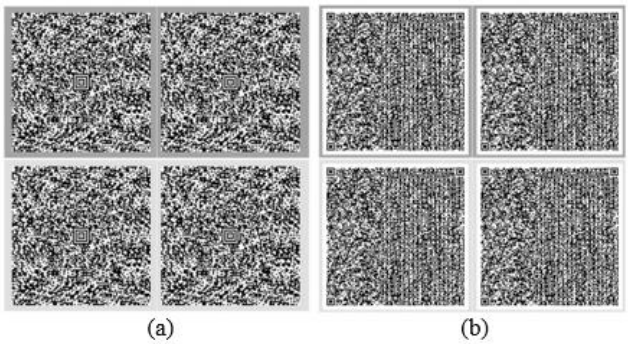
Tablo 1. Önerilen yaklaşımda kullanılan parametreler ve değerleri

Model/Yöntem	Parametre	Tercih/Değer
DeiT3	Devir (Epoch) sayısı	10
	Öğrenme Oranı	1e-4
	Optimizasyon	SGD
Swin	Aktivasyon Fonksiyonu	Linear
	Kayıp Fonksiyonu	Cross Entropy Loss
	Donanım Kaynağı	Tekli GPU
MaxVİT	Mini-topluluk(mini-batch)	14
	Eğitim Oranı: Test Oranı	%70:%30
kNN	Ön Ayar	Fine kNN
	Komşu Sayısı	1
	Mesafe Ölçüsü	Euclidean
	Mesafe Ağırlığı	Equal
	Standart Veri	True
SVM	Ön Ayar	Cubic SVM
	Çekirdek Fonksiyonu	Cubic
	Çekirdek Ölçeği	Automatic
	Kutu Kısıtlama Düzeyi	1
	Çoklu Sınıf Yöntemi	One-vs-One
	Standart Veri	True

Deneysel çalışmalar üç aşamadan oluşmuştur. İlk aşamada, kullanılan veri kümesi çeşitli önişlem adımlarına tabi tutulmuştur. Bu aşamanın temel amacı, 1B verilerin 2B barkod formatlarına dönüştürülmesi ve böylece elde edilen verilerin 2B tabanlı derin öğrenme modelleri ile eğitilmesidir. Bu yaklaşım sayesinde, verilerin daha anlamlı ve ayırt edici özellikler kazanması ve sonraki sınıflandırma

süreçlerinde model performansının artırılması hedeflenmiştir.

Önişlem aşamasında özellikle Aztec ve QR kodlama teknikleri kullanılmış, bu yöntemlerle 1B verilerden görsel temsiller üretilmiştir. Bu temsiller, veri çeşitliliğini artırmakta ve modelin karmaşık desenleri daha etkili biçimde öğrenmesine katkı sağlamıştır. Çalışmada kullanılan örnek görüntü kümesi ise Şekil 6'da sunulmuştur.

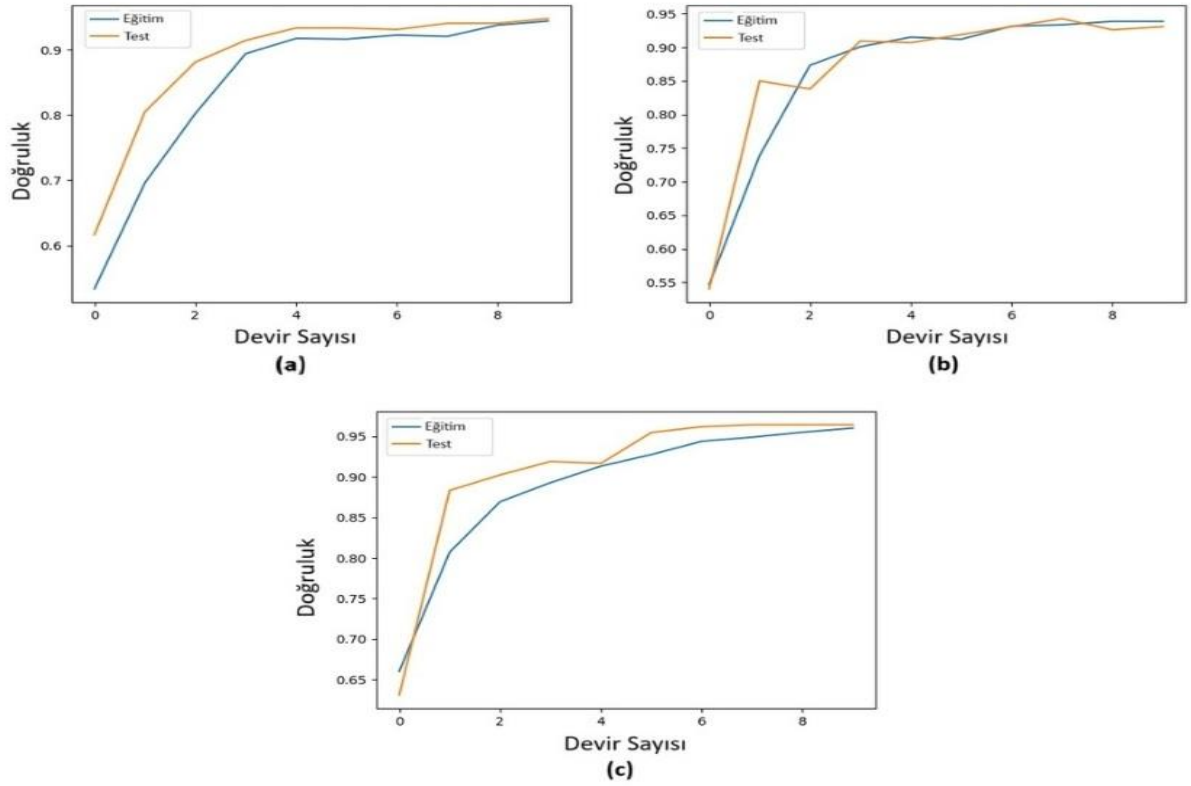


Şekil 6. Veri kümesine ait barkod görüntü örnekleri a) Aztec görüntü kümesi, b) QR görüntü kümesi

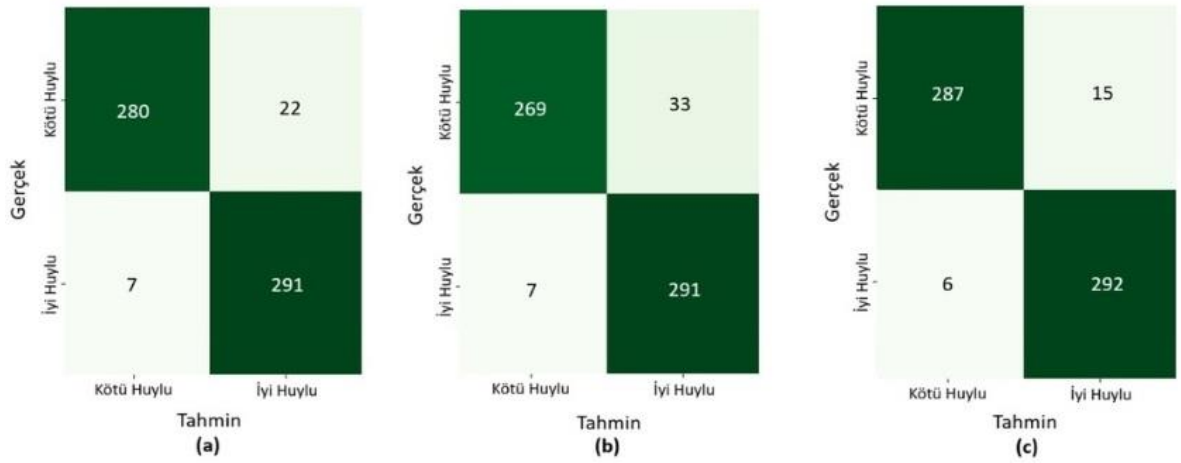
Deneysel analizin ikinci adımında 2B veri kümeleri (Aztec, QR) tranformer modeller (DeiT3, MaxViT, Swin) ile eğitilmiştir. Burada veri kümesinin %30'u test verisi olarak ayrılmıştır. Aztec tabanlı veri kümesinin model eğitimlerinden elde edilen başarı grafikleri Şekil 7'de gösterilmiştir ve elde edilen karmaşıklık matrisleri Şekil 8'de gösterilmiştir. Karmaşıklık matrislerinin metrik analiz sonuçları Tablo 2'de gösterilmiştir.

Tablo 2'de, Aztec tabanlı veri kümesi üzerinde elde edilen karmaşıklık matrislerinin metrik analiz sonuçları gösterilmiştir. Sonuçlar incelendiğinde, Swin modeli %96.50 doğruluk oranı ile en yüksek başarıya ulaşmıştır.

Bu model, hem iyi huylu sınıfta %95 kesinlik, %97 geri çağırma ve %96 F1 skoru, hem de kötü huylu sınıfta %97 kesinlik, %95 geri çağırma ve %96 F1 skoru ile dengeli bir performans sergilemiştir. DeiT3 modeli %95.17 doğruluk oranı ile ikinci sırada yer almıştır. DeiT3 modeli iyi huylu sınıfta %93 kesinlik, %98 geri çağırma ve %95 F1 skoru; kötü huylu sınıfta ise %97 kesinlik, %92 geri çağırma ve %95 F1 skoru ile başarılı bir performans ortaya koymuştur. MaxViT modeli ise %93.33 doğruluk oranı ile diğer modellere kıyasla daha düşük sonuçlar elde etmiş, iyi huylu sınıfta %90 kesinlik ve %98 geri çağırma ile %93 F1 skoru, kötü huylu sınıfta ise %97 kesinlik, %89 geri çağırma ve %93 F1 skoru üretmiştir. Genel olarak değerlendirildiğinde, Aztec tabanlı veri kümesi üzerinde Swin modelinin diğer modellere kıyasla daha kararlı ve yüksek performans gösterdiği, DeiT3'ün yakın sonuçlarla ikinci sırada yer aldığı ve MaxViT'in ise görece daha sınırlı bir başarıya sahip olduğu söylenebilir.



Şekil 7. Aztec tabanlı veri kümesinin transformer modellerine ait eğitim ve test başarı grafikleri (a) DeiT3, (b) MaxViT, (c) Swin



Şekil 8. Aztec tabanlı veri kümesi kullanılarak elde edilen transformer modellerine ait karmaşıklık matrisleri (a) DeiT3, (b) MaxViT, (c) Swin

Tablo 2. Aztec tabanlı veri kümesine ait karmaşıklık matrislerinin metrik analiz sonuçları

Ön İşlem	Model	Sınıf	Kesinlik	Geri Çağırma	F1 Skoru	Doğruluk	Genel Doğruluk (%)
Aztec	DeiT3	İyi Huylu	0.93	0.98	0.95	0.95	95.17
		Kötü Huylu	0.97	0.92	0.95	0.95	
	MaxVİT	İyi Huylu	0.90	0.98	0.93	0.93	93.33
		Kötü Huylu	0.97	0.89	0.93	0.93	
	Swin	İyi Huylu	0.95	0.97	0.96	0.96	96.50
		Kötü Huylu	0.97	0.95	0.96	0.96	

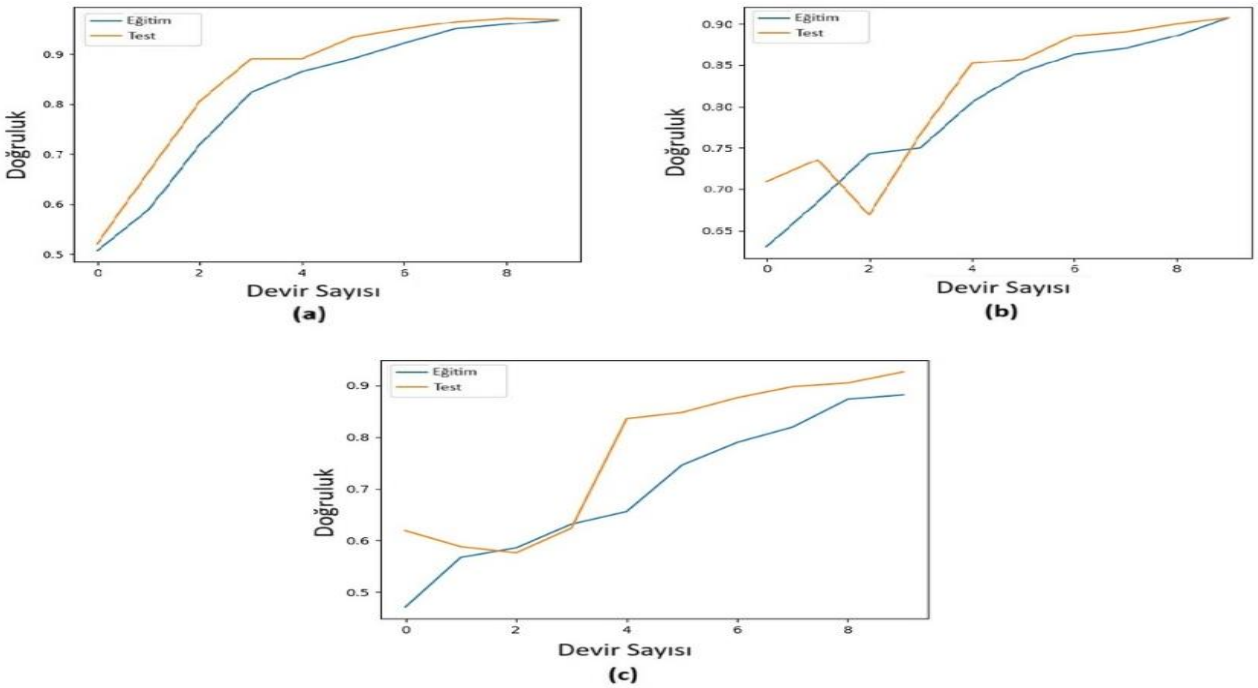
Deneysel analizin ikinci aşamasında kullanılan diğer veri kümesi olan QR tabanlı veri kümesine ait model eğitim sonuçları Şekil 9'da sunulmuştur. Bu eğitimlerden elde edilen karmaşıklık matrisleri ise Şekil 10'da verilmiştir. Söz konusu matrislerden türetilen metrik analiz sonuçları ise Tablo 3'te ayrıntılı olarak gösterilmiştir.

Tablo 3'te, QR tabanlı veri kümesi üzerinde elde edilen karmaşıklık matrislerinin metrik analiz sonuçları sunulmuştur. Bulgular incelendiğinde, DeiT3 modeli %95.50 doğruluk oranı ile en yüksek başarıya ulaşmıştır. Model, iyi huylu sınıfta %93 kesinlik, %98 geri çağırma ve %95 F1 skoru; kötü huylu sınıfta ise %98 kesinlik, %92 geri çağırma ve %95 F1 skoru ile dengeli bir performans sergilemiştir. MaxViT modeli %90.17 doğruluk oranı ile daha düşük bir başarı göstermiş olup, iyi huylu sınıfta %87 kesinlik ve %92 geri çağırma ile %90 F1 skoru, kötü huylu sınıfta ise %92 kesinlik, %87 geri çağırma ve %89 F1 skoru elde etmiştir. Swin modeli ise %92.17 doğruluk oranı ile orta seviyede bir sonuç üretmiş, iyi huylu sınıfta %88 kesinlik, %97 geri çağırma ve %92 F1 skoru ile öne çıkarken; kötü huylu sınıfta %97 kesinlik, %87 geri çağırma ve %91 F1 skoru ile görece daha sınırlı bir performans sergilemiştir. Genel olarak, QR tabanlı veri kümesinde DeiT3 modelinin diğer modellere kıyasla daha kararlı ve yüksek bir performans ortaya koyduğu, MaxViT ve Swin'in ise özellikle kötü huylu sınıfta daha düşük geri çağırma değerleri nedeniyle daha sınırlı bir başarı göstermiştir.

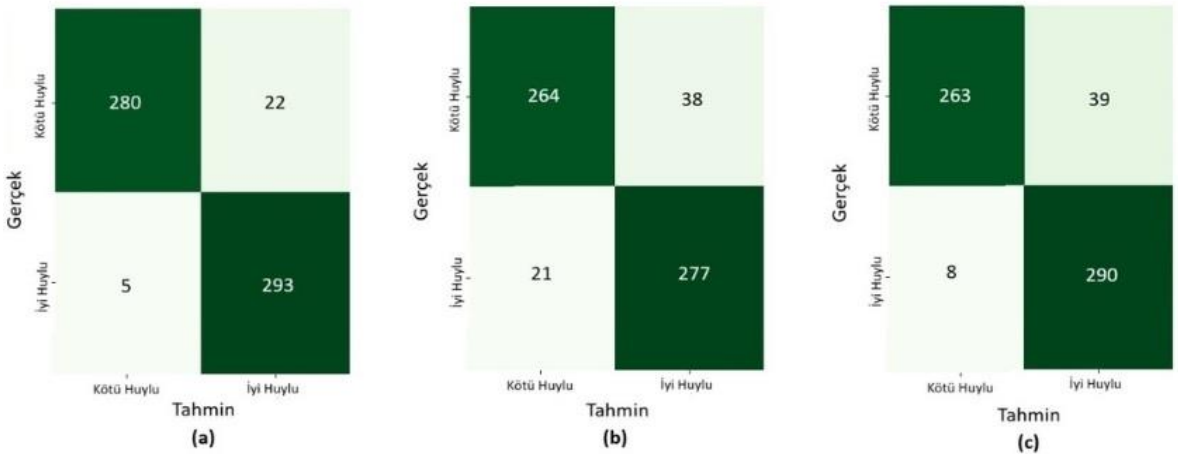
Deneysel analizin üçüncü aşamasında model eğitimlerinden elde edilen özellik setleri arasından en yüksek başarıyı gösteren ilk üç set seçilmiştir. Bu setler ve temsil sembolleri şu şekilde belirlenmiştir: A (Aztec–DeiT3), B (Aztec–Swin), C (QR–DeiT3). Sürecin devamında, bu setler üzerinde özellik füzyonu tekniği uygulanmış ve setler farklı kombinasyonlarla birleştirilmiştir. Oluşturulan birleşim kümeleri A&B (Aztec-DeiT3&Aztec-Swin), A&C (Aztec-DeiT3&QR-DeiT3), B&C (Aztec-Swin&QR-DeiT3) ve A&B&C (Aztec-DeiT3&Aztec-Swin&QR-DeiT3) şeklindedir.

'A&B' birleşiminden 1792, 'A&C'den 1536, 'B&C'den 1792 ve 'A&B&C'den 2560 özellik sütunu elde edilmiştir. Elde edilen bu özellik setleri, sınıflandırma aşamasında kNN ve SVM yöntemleri ile değerlendirilmiştir. kNN sınıflandırıcısı kullanılarak elde edilen karmaşıklık matrisleri Şekil 11'de, ilgili metrik sonuçlar ise Tablo 4'te sunulmuştur. Ayrıca özellik setleri çapraz doğrulama (k=5) tekniği kullanarak analizler gerçekleşmiş ve analiz sonuçları Tablo 5'te gösterilmiştir.

Bulgular incelendiğinde, tüm kombinasyonlarda yüksek doğruluk oranlarının elde edildiği ve sınıflandırma performansının oldukça tutarlı olduğu görülmüştür. Özellikle A&C özellik kümesi, eğitim-test veri tekniğine göre %98 doğruluk; çapraz doğrulama tekniğine göre doğruluk ile en başarılı sonucu vermiştir. Bu durum, farklı barkod tiplerinden türetilen özelliklerin birlikte kullanımının sınıflar arası ayrımı güçlendirdiğini göstermiştir.



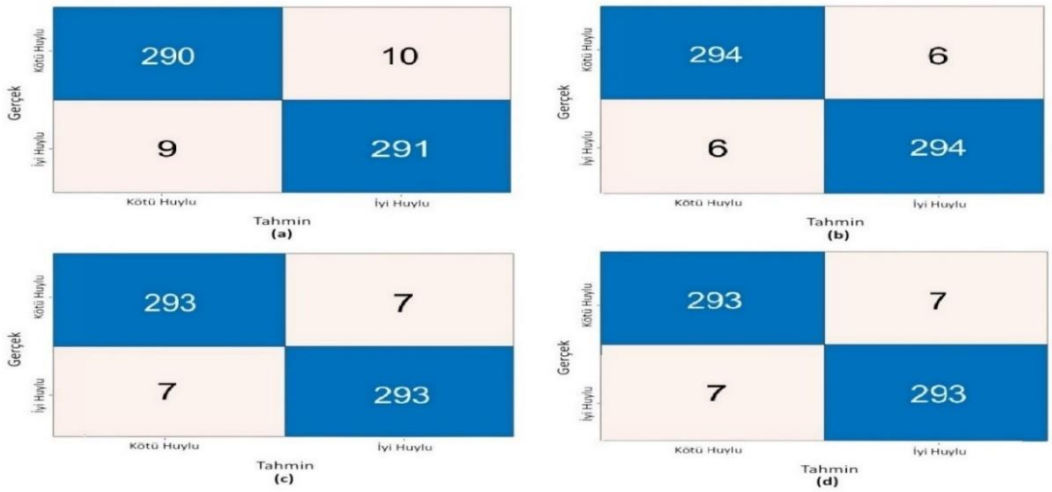
Şekil 9. QR tabanlı veri kümesinin transformer modellerine ait eğitim ve test başarı grafikleri (a) DeiT3, (b) MaxViT, (c) Swin



Şekil 10. QR tabanlı veri kümesi kullanılarak elde edilen transformer modellerine ait karmaşıklık matrisleri (a) DeiT3, (b) MaxViT, (c) Swin

Tablo 3. QR tabanlı veri kümesine ait karmaşıklık matrislerinin metrik analiz sonuçları

Ön İşlem	Model	Sınıf	Kesinlik	Geri Çağırma	F1 Skoru	Doğruluk	Genel Doğruluk (%)
QR	DeiT3	İyi Huylu	0.93	0.98	0.95	0.95	95.50
		Kötü Huylu	0.98	0.92	0.95	0.95	
	MaxVİT	İyi Huylu	0.87	0.92	0.90	0.90	90.17
		Kötü Huylu	0.92	0.87	0.89	0.90	
	Swin	İyi Huylu	0.88	0.97	0.92	0.92	92.17
		Kötü Huylu	0.97	0.87	0.91	0.92	



Şekil 11. Özellik füzyon tekniği ile elde edilmiş özellik setlerinin kNN yöntemi ile sınıflandırılması sonucu elde edilen karmaşıklık matrisleri a) A&B, b) A&C, c) B&C, d) A&B&C

Tablo 4. Özellik füzyon tekniği ile elde edilmiş özellik setlerinin kNN yöntemi ile sınıflandırılması sonucu elde edilen karmaşıklık matrislerinin metrik sonuçları (eğitim-test tekniği ile)

Yöntem	Set Birleştirme	Sınıf	Kesinlik	Geri Çağırma	F1 Skoru	Doğruluk	Genel Doğruluk (%)
kNN	A&B	İyi Huylu	0.96	0.97	0.96	0.96	96.83
		Kötü Huylu	0.96	0.96	0.96	0.96	
	A&C	İyi Huylu	0.98	0.98	0.98	0.98	98.0
		Kötü Huylu	0.98	0.98	0.98	0.98	
	B&C	İyi Huylu	0.97	0.97	0.97	0.97	97.67
		Kötü Huylu	0.97	0.97	0.97	0.97	
	A&B&C	İyi Huylu	0.97	0.97	0.97	0.97	97.67
		Kötü Huylu	0.97	0.97	0.97	0.97	

Tablo 5. Özellik füzyon tekniği ile elde edilmiş özellik setlerinin kNN yöntemi ile sınıflandırılması sonucu elde edilen karmaşıklık matrislerinin metrik sonuçları (çapraz doğrulama tekniği ile k=5)

Yöntem	Set Birleştirme	Sınıf	Kesinlik	Geri Çağırma	F1 Skoru	Doğruluk	Genel Doğruluk (%)
kNN	A&B	İyi Huylu	0.95	0.96	0.95	0.95	95.80
		Kötü Huylu	0.95	0.95	0.95	0.95	
	A&C	İyi Huylu	0.97	0.97	0.97	0.97	97.10
		Kötü Huylu	0.97	0.97	0.97	0.97	
	B&C	İyi Huylu	0.96	0.96	0.96	0.96	96.50
		Kötü Huylu	0.96	0.96	0.96	0.96	
	A&B&C	İyi Huylu	0.96	0.96	0.96	0.96	96.40
		Kötü Huylu	0.96	0.96	0.96	0.96	

Tablo 4 ve Tablo 5'teki diğer özellik setleri (A&B, B&C ve A&B&C) incelendiğinde %95 ile %98 arasında değişen doğruluk değerleriyle başarılı performanslar sergilemiştir. Genel olarak değerlendirildiğinde, kNN yöntemi ile gerçekleştirilen sınıflandırmalarda özellik füzyonunun etkinliği doğrulanmış ve özellikle A&C birleşiminin sınıflandırma başarısında öne çıktığı ortaya konulmuştur.

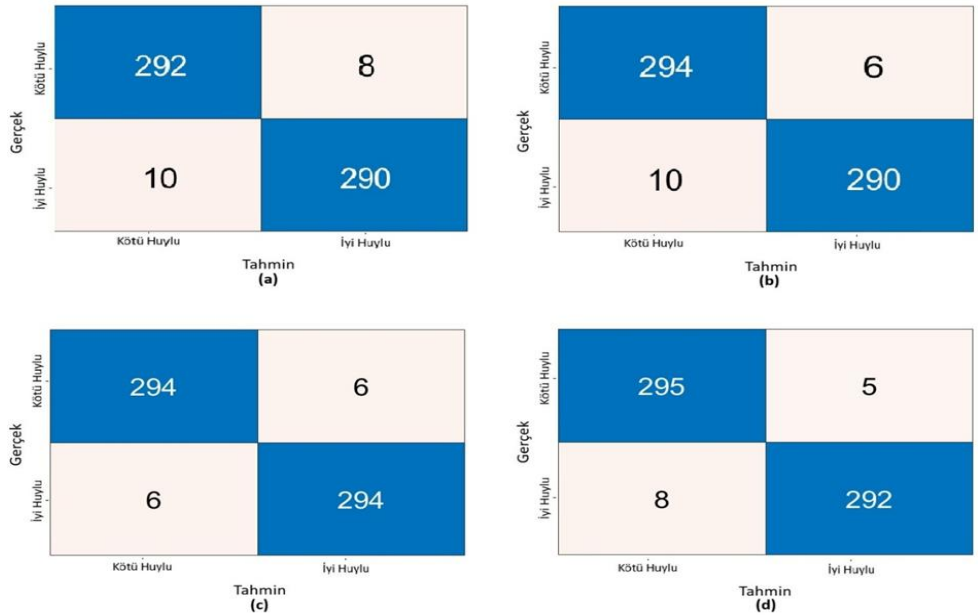
SVM sınıflandırıcısı ile gerçekleştirilen analizlerde de farklı özellik seti kombinasyonları değerlendirilmiştir. Şekil 12'de SVM algoritmasına ait karmaşıklık matrisleri, Tablo 6'da ise elde edilen metrik değerler sunulmuştur. Ayrıca özellik setleri çapraz doğrulama (k=5) tekniği kullanarak analizler gerçekleşmiş ve analiz sonuçları Tablo 7'de gösterilmiştir.

Elde edilen bulgular, tüm set birleşimlerinde yüksek doğruluk oranlarına ulaşıldığını göstermiştir. Özellikle B&C özellik kümesi, eğitim-test tekniği ile %98 doğruluk; çapraz doğrulama tekniği ile %97.50 doğruluk ile en başarılı sonucu vermiştir. Bu durum, farklı barkod tiplerinden çıkarılan özelliklerin birlikte değerlendirilmesinin sınıflar arası ayrımı güçlendirdiğini ortaya koymuştur. Diğer kombinasyonlarda da benzer

şekilde yüksek performans değerleri elde edilmiştir. Tablo 6 incelendiğinde, A&B ve A&C birleşimlerinde sırasıyla %97 ve %97.33 doğruluk elde edilmiş, çoklu birleşim olan A&B&C setinde ise %97.83 doğruluk elde edilmiştir. Benzer sonuçlar Tablo 7 incelendiğinde çapraz doğrulama tekniğiyle de elde edilmiştir. Bu bulgular, SVM algoritmasının yüksek boyutlu özellik uzayında kararlı sınıflandırma yapabilme kapasitesini desteklemiştir. Genel olarak değerlendirildiğinde, SVM ile gerçekleştirilen analizler, önerilen özellik füzyonu yaklaşımının sınıflandırma performansını anlamlı ölçüde artırmış ve güvenilir sonuçlar sağlamıştır.

4 Tartışma

Bu çalışmada, kötü amaçlı yazılımların tespiti için barkod tabanlı görselleştirme ile transformer modellerinin birlikte kullanıldığı bir yaklaşım geliştirilmiştir. Elde edilen sonuçlar, özellikle QR ve Aztec kodları üzerinden çıkarılan özniteliklerin kNN ve SVM algoritmalarıyla sınıflandırılmasında yüksek doğruluk sağlamıştır. Bu durum, metin tabanlı kötü amaçlı yazılım verilerinin görsel



Şekil 12. Özellik füzyon tekniği ile elde edilmiş özellik setlerinin SVM yöntemi ile sınıflandırılması sonucu elde edilen karmaşıklık matrisleri a) A&B, b) A&C, c) B&C, d) A&B&C

Tablo 6. Özellik füzyon tekniği ile elde edilmiş özellik setlerinin SVM yöntemi ile sınıflandırılması sonucu elde edilen karmaşıklık matrislerinin metrik sonuçları (eğitim-test tekniği ile)

Yöntem	Set Birleştirme	Sınıf	Kesinlik	Geri Çağırma	F1 Skoru	Doğruluk	Genel Doğruluk (%)
SVM	A&B	İyi Huylu	0.97	0.96	0.96	0.97	97.0
		Kötü Huylu	0.96	0.97	0.97	0.97	
	A&C	İyi Huylu	0.97	0.96	0.97	0.97	97.33
		Kötü Huylu	0.96	0.98	0.97	0.97	
	B&C	İyi Huylu	0.98	0.98	0.98	0.98	98.0
		Kötü Huylu	0.98	0.98	0.98	0.98	
	A&B&C	İyi Huylu	0.98	0.97	0.97	0.97	97.83
		Kötü Huylu	0.97	0.98	0.97	0.97	

Tablo 7. Özellik füzyon tekniği ile elde edilmiş özellik setlerinin SVM yöntemi ile sınıflandırılması sonucu elde edilen karmaşıklık matrislerinin metrik sonuçları (çapraz doğrulama tekniği ile k=5)

Yöntem	Set Birleştirme	Sınıf	Kesinlik	Geri Çağırma	F1 Skoru	Doğruluk	Genel Doğruluk (%)
SVM	A&B	İyi Huylu	0.96	0.95	0.95	0.96	96.0
		Kötü Huylu	0.95	0.96	0.96	0.96	
	A&C	İyi Huylu	0.96	0.95	0.96	0.96	96.33
		Kötü Huylu	0.96	0.97	0.96	0.96	
	B&C	İyi Huylu	0.97	0.97	0.97	0.97	97.50
		Kötü Huylu	0.97	0.98	0.98	0.97	
	A&B&C	İyi Huylu	0.97	0.96	0.96	0.97	96.70
		Kötü Huylu	0.96	0.97	0.96	0.97	

Tablo 8. Önerilen yaklaşımın diğer çalışmalar ile karşılaştırılması

Çalışma	Kullanılan Yöntem	Özellik İşleme	Sınıflandırıcılar	Genel Doğruluk (%)
Kattamuri ve ark.	Sürü Optimizasyonu	Optimizasyon tabanlı öznitelik seçimi	Random Forest, XGBoost, LightGBM, CatBoost	99.97
Bu çalışma	1D verilerin QR ve Aztec barkodlarına dönüştürülmesi	Transformer tabanlı öznitelik çıkarımı + Özellik Füzyonu	kNN, SVM	98

forma dönüştürülmesinin, sınıflandırma sürecinde önemli avantajlar sunduğunu ortaya koymuştur. Önerilen yöntemin güçlü yönlerinden biri, özellik füzyonu sayesinde farklı barkod ve model kombinasyonlarından elde edilen özniteliklerin bir arada kullanılmasıdır. Bu sayede tek bir modelden elde edilebilecek sınırlı temsili aşarak, sınıflandırma başarısını artırmıştır. Ayrıca kNN ve SVM algoritmalarıyla gerçekleştirilen sınıflandırma süreci, hem hesaplama açısından daha verimli olmuş hem de sonuçların yorumlanabilirliğini artırmıştır.

Deneysel analizler de özellik füzyonu performans sonuçlarını olumlu etkilemiştir. Ayrıca makine öğrenme yöntemlerinin seçimi de sonuçları etkileyen bir diğer faktördür. Nitekim (B&C) özellik setinde en iyi performansı SVM ile %98 elde etmişken, kNN yöntemi ile en iyi performansı (A&C) özellik füzyon setiyle edilmiş ve bu sette %98 genel doğruluk başarısı sağlanmıştır. Burada hem özellik füzyonu hem de makine öğrenme yöntemlerinin katkıları net gözlemlenmiştir.

Aynı veri kümesini kullanarak analizler gerçekleştiren diğer çalışmaların analiz özeti Tablo 8'de verilmiştir. Kattamuri ve arkadaşları çalışmalarında, Somlap veri kümesi üzerinde sürü zekâsı tabanlı optimizasyon yöntemleri ve makine öğrenmesi algoritmalarını bir arada kullanmışlardır. Özellik seçimi için karınca kolonisi optimizasyonu uygulanmış ve seçilen öznitelikler, XGBoost, Random Forest, LightGBM ve CatBoost gibi sınıflandırıcılarla değerlendirilmiştir. Çalışmanın sonucunda, özellikle XGBoost algoritması ile %99.37 doğruluk oranı elde edilmiştir [9]. Bu sonuç, özellik seçiminin model performansına katkı sağladığını ve topluluk öğrenme yöntemlerinin zararlı yazılım tespitinde oldukça etkili olduğunu göstermektedir. Ancak bu tür yöntemler yüksek hesaplama maliyeti ve geniş veri işleme gereksinimi taşırken, bu çalışmada barkod tabanlı görselleştirme ve transformer modellerinin entegrasyonu ile daha yenilikçi ve esnek bir çözüm ortaya konulmuştur. Böylece, %98 başarı oranı yalnızca sayısal bir gösterge değil, aynı zamanda yöntemin pratik uygulanabilirliğini ve literatüre getirdiği özgün katkıyı yansıtan önemli bir bulgu niteliği taşımıştır.

Bununla birlikte, çalışmanın bazı sınırlılıkları bulunmaktadır. Öncelikle, yalnızca QR ve Aztec barkod türleri kullanılmış ve analizler rastgele seçilen 1000 örnek üzerinden gerçekleştirilmiştir. Daha geniş örneklem setleri ve farklı barkod türlerinin eklenmesi, yöntemin genellenebilirliğini artırabilir. Donanımsal desteğin sınırlı olmasından dolayı deneysel analizler belirtilen ölçüler çerçevesinde gerçekleşmiştir. Ayrıca uçtan uca bir model tasarımı gerçekleştirilebilseydi zaman kazancı sağlatılabilirdi. Bir sonraki çalışmalarda bu sınırlılıklar göz önünde bulundurularak önerilen yaklaşım geliştirilecektir.

5 Sonuç ve öneriler

Son yıllarda dijital ortamların yaygınlaşmasıyla birlikte kötü amaçlı yazılımlar daha büyük bir tehdit haline gelmiştir. Geleneksel imza tabanlı yöntemler, yalnızca önceden bilinen saldırıları tespit edebildiği için yeni ve karmaşık yazılımların yakalanmasında yetersiz kalmaktadır. Bu nedenle, bilgi güvenliği alanında daha esnek ve güçlü yöntemlerin geliştirilmesine ihtiyaç duyulmaktadır. Yapay zekâ ve veri görselleştirme tabanlı yaklaşımlar, bu ihtiyacı karşılamada öne çıkan yöntemler arasında yer almaktadır.

Bu çalışmada, kötü amaçlı yazılım tespitine yönelik olarak barkod tabanlı görselleştirme ve transformer mimarilerini bir araya getiren hibrit bir yöntem geliştirilmiştir. Somlap veri kümesinden elde edilen 1B veriler QR ve Aztec barkodlarına dönüştürülmüş, bu görseller üzerinden DeiT3, MaxViT ve Swin transformer modelleri ile öznitelik çıkarımı gerçekleştirilmiştir. Özellik füzyonu ile birleştirilen öznitelikler, kNN ve SVM algoritmalarıyla sınıflandırılmış ve yüksek doğruluk oranlarına ulaşılmıştır.

Elde edilen bulgular, barkod tabanlı temsillerin, kötü amaçlı yazılım örneklerinin görsel açıdan daha zengin ve yoğun bir şekilde incelenmesine imkân tanıdığını göstermiştir. Transformer tabanlı modellerin güçlü öznitelik çıkarım kapasiteleri ve makine öğrenmesi algoritmalarının esnek sınıflandırma yetenekleri bir araya geldiğinde, literatürdeki birçok yönteme kıyasla daha başarılı sonuçlar elde edilmiştir.

Bununla birlikte, çalışmada yalnızca QR ve Aztec barkodlarının değerlendirilmesi ve sınıflandırmada kNN ile SVM algoritmalarıyla sınırlı kalınması, yöntemin çeşitliliğini kısıtlamaktadır. Daha geniş veri kümeleri, farklı barkod türleri ve alternatif sınıflandırma algoritmalarıyla yapılacak deneyler yöntemin genellenebilirliğini artıracaktır.

Gelecek araştırmalarda, bu yaklaşımın farklı platformlarda uygulanabilirliği, gerçek zamanlı sistemlere entegrasyonu ve diğer güvenlik çözümleriyle bütünleştirilmesi hedeflenmektedir. Bu tür hedefler, yöntemin hem akademik hem de endüstriyel anlamda katkı potansiyelini artıracağı öngörülmektedir.

Çıkar çatışması

Yazarlar çıkar çatışması olmadığını beyan etmektedir.

Benzerlik oranı (iThenticate): %8

Burada makalenin benzerlik oranı beyan edilmelidir.

Bilgilendirme

Bu makale Fırat Üniversitesi Sosyal Bilimler Enstitüsü tarafından yürütülen "Kötü Amaçlı Yazılımların Transformer Modelleriyle Tespiti: 1B Verilerin 2B Barkod Türlerine Dönüştürülmesi" adlı yüksek lisans tezine dayanmaktadır.

Kaynaklar

[1] J. Ferdous, R. Islam, A. Mahboubi, and M. Z. Islam, A survey on ML techniques for multi-platform malware detection: securing PC, mobile devices, IoT, and cloud environments. Sensors, 25(4), 1153, 2024. https://doi.org/10.3390/s25041153

[2] E. Muhati and D. Rawat, Data driven network anomaly detection with cyber attack and defense visualization. Journal of Cybersecurity and Privacy, 4(2), 241–263, 2024. https://doi.org/10.3390/jcp4020012.

[3] F. Ullah, H. Naeem, A. Rauf, and A. Almogren, Explainable malware detection system using transformer-based transfer learning and multi-model visual representation. Sensors, 22(18), 6766, 2023. https://doi.org/10.3390/s22186766.

[4] A. Alqahtani, W. Z. Khan, and S. S. Alshamrani, Web-based malware detection system using convolutional neural network. Digital, 3(3), 273–285, 2023. https://doi.org/10.3390/digital3030017.

[5] M. Ashawa, J. Lee, and S. Kim, Enhanced image-based malware classification using transformer-based CNNs. Electronics, 13(20), 4081, 2024. https://doi.org/10.3390/electronics13204081.

[6] J. Xue, C. Lin, Y. Liu, and Y. Guo, MC-ISA: a multi-channel code visualization method for malware detection. Electronics, 12(10), 2272, 2023. https://doi.org/10.3390/electronics12102272.

[7] A. A. Hafeth and A. I. Abdullahi, An efficient malware detection method using a hybrid ResNet-transformer network and IGOA-based wrapper feature selection (HRT-Net). Electronics, 14(13), 2741, 2025. https://doi.org/10.3390/electronics14132741.

[8] L. Qian and L. Cong, Channel features and API frequency-based transformer model for malware identification. Sensors, 24(2), 580, 2022. https://doi.org/10.3390/s24020580.

[9] S. J. Kattamuri, R. K. V. Penmatsa, S. Chakravarty, and V. S. P. Madabathula, Swarm optimization and machine learning applied to PE malware detection towards cyber threat intelligence. Electronics, 12(2), 342, 2023. https://doi.org/10.3390/electronics12020342.

[10] R. K. Varma, SOMLAP data set. Kaggle, https://www.kaggle.com/datasets/ravikiranvarmap/somlap-data-set, 2025.

[11] C. Center, Aztec codes. https://www.cognex.com/resources/symbologies/2-d-matrix-codes/aztec-codes (Erişim tarihi: 12.03.2023).

[12] J. Yi, L. Chen, Y. Zhang, and H. Wu, Enhancement of two-dimensional barcode restoration techniques. Electronics, 13(10), 1873, 2024. https://doi.org/10.3390/electronics13101873.

[13] Y. Wang, Vision transformers for image classification. Technologies, 13(1), 32, 2025. https://doi.org/10.3390/technologies13010032

[14] J. Zhao, T. Liu, and L. Sun, Multi-scale fusion MaxViT for medical image classification. Electronics, 14(5), 912, 2025. https://doi.org/10.3390/electronics14050912.

[15] F. Zheng, S. Lin, W. Zhou, and H. Huang, A lightweight dual-branch Swin transformer for remote sensing scene classification. Remote Sensing, 15(11), 2865, 2023. https://doi.org/10.3390/rs15112865.

[16] A. Çetinkaya, Analysis of machine learning classification approaches. Sustainability, 15(17), 12917, 2023. https://doi.org/10.3390/su151712917.

[17] H. Babbar et al., Detection of android malware in the internet of things using KNN and static-dynamic analysis. Sensors, 23(16), 7256, 2023. https://doi.org/10.3390/s23167256.

[18] N. Aldhafferi, Android malware detection using support vector regression for dynamic feature analysis. Information, 15(10), 658, 2024. https://doi.org/10.3390/info15100658.

[19] I. Markoulidakis, G. Kopsiaftis, I. Rallis, and I. Georgoulas, Multi-class confusion matrix reduction method and its application on net promoter score classification problem. Proceedings of the 14th Pervasive Technologies Related to Assistive Environments Conference, 412–419, 2021. https://doi.org/10.3390/technologies9040081.

[20] A. Çalışkan, Detecting human activity types from 3D posture data using deep learning models. Biomedical Signal Processing and Control, 81, 104479, 2023. https://doi.org/10.1016/j.bspc.2022.104479.

[21] Y. Wang, Y. Jia, Y. Tian, and J. Xiao, Deep reinforcement learning with the confusion-matrix-based dynamic reward function for customer credit scoring. Expert Systems with Applications, 200, 117013, 2022. https://doi.org/10.1016/j.eswa.2022.117013.

[22] Y. E. Gür, M. Toğaçar, and B. Solak, Integration of CNN models and machine learning methods in credit score classification: 2D image transformation and feature extraction. Computational Economics, 65(5), 2991–3035, 2025. https://doi.org/10.1007/s10614-025-10893-5.