Adıyaman University
Journal of Engineering Sciences
Adyü J Eng Sci 2026;13:e260113
Adıyaman Üniversitesi
Mühendislik Bilimleri Dergisi
Adyü Müh Bil Derg 2026;13:e260113
https://doi.org/10.54365/adyumbd.1805519

Research Article / Araştırma Makalesi

Fidye Yazılımlarında Anomali ve Sahte İmza Tespiti: Zaman-Frekans Dönüşümü ve Transformer Tabanlı Analiz Modeli

Ransomware Anomaly and Fake Signature Detection: Time-Frequency Transform and Transformer-Based Analysis Model

Burak Alperen Bahçeci [1]*, Mesut Toğaçar [2]

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

Öz

Günümüzde siber güvenlik alanında fidye yazılımları, veri gizliliği ve bütünlüğü açısından en kritik tehditlerden biri haline gelmiştir. Bu tür zararlı yazılımlar, sistemlere sızarak önemli verileri şifreler, kullanıcı erişimini engeller ve hem bilgi güvenliği hem de ekonomik istikrar üzerinde ciddi tehditler oluşturur. Bu çalışmada, fidye yazılımlarının tespiti için zaman-frekans dönüşümlerine dayalı yeni bir analiz yaklaşımı önerilmektedir. Gerçek dünyadan elde edilen açık erişimli bir veri kümesi kullanılarak bir boyutlu veriler dalgacık dönüşüm teknikleriyle iki boyutlu spektral görüntülere dönüştürülmüştür. Bu görüntüler Vision Transformer modeliyle eğitilmiş, elde edilen özellik setleri incelenmiştir. En yüksek performansı gösteren özellikler, mRMR ve Relief yöntemleriyle seçilerek sınıflandırma başarısına etkileri analiz edilmiştir. Seçilen özellik setlerinin birleştirilmesiyle oluşturulan yapı, Naif Bayes sınıflandırıcısı kullanılarak değerlendirilmiştir. Elde edilen %99.3 doğruluk oranı çapraz doğrulama yöntemiyle teyit edilmiştir. Sonuçlar, önerilen yaklaşımın fidye yazılımlarını geleneksel yöntemlere göre daha yüksek doğrulukla tespit ettiğini göstermektedir.

Anahtar Kelimeler: *Sahte imza tespiti, Siber Saldırı, Transformer öğrenme, Anomali tespiti, Dalgacık dönüşüm.*

Abstract

In recent years, ransomware has emerged as one of the most critical threats in the field of cybersecurity, particularly with respect to data privacy and integrity. Such malicious software infiltrates systems, encrypts sensitive data, restricts user access, and poses serious risks to both information security and economic stability. In this study, a novel analysis approach based on time–frequency transformations is proposed for ransomware detection. Using a real-world, publicly available dataset, one-dimensional data are transformed into two-dimensional spectral images through wavelet-based transformation techniques. These images are used to train a Vision Transformer model, and the resulting feature sets are examined. The features yielding the highest performance are selected using the mRMR and Relief algorithms, and their impact on classification performance is analyzed. The structure formed by combining the selected feature sets is evaluated using a Naive Bayes classifier. The achieved classification accuracy of 99.3% is validated through a cross-validation methodology. The results demonstrate that the proposed approach detects ransomware with higher accuracy compared to traditional methods.

Keywords: *Fake signature detection, Cyber attack, Transformer learning, Anomaly detection, Wavelet transformatio n.*

* Sorumlu yazar e-posta (Corresponding e-mail): burakbahceci06@gmail.com
Geliş Tarihi (Received):17.10.2025, **Kabul Tarihi (Accepted):** 24.03.2026

1. Giriş

Siber güvenlik, bilişim altyapılarını, iletişim kanallarını ve verileri korumaya yönelik araçlar ile stratejik yaklaşımların araştırılmasıyla ilgilenen bir disiplindir. Bu alandaki en kritik meselelerden biri, dijital sistemlere zarar verme amacı güden planlı müdahaleleri ifade eden siber tehlikelerdir [1]. Dijital teknolojilerin sağlık, iletişim, sanayi ve eğitim gibi stratejik sektörlerde köklü dönüşümler yaratması, çağımızda siber güvenliğin temel unsurlardan biri olarak konumlanmasına neden olmuştur. 21. yüzyıla yaklaşan süreçte, Türkiye'nin de içinde bulunduğu birçok ülkede dijital tehdit unsurları, bireysel düzeyde değerlendirilen yasa dışı eylemler arasında yer almaya başlamıştır. Bilgi sistemlerine yönelik artan saldırılar, devlet güvenliğini etkileyen unsurlar kapsamında ele alınarak bu tür dijital eylemler, kamu güvenliğine karşı yapılan tehdit kategorisine dahil edilmiş ve bu riskleri azaltmaya yönelik koruyucu yapıların oluşturulması hedeflenmiştir. Saldırı girişiminde bulunanlar gizli içeriklere ulaşmak ya da bu verileri ifşa etmek amacıyla zararlı kodlar, şifreleme temelli fidye yazılımları, insan odaklı aldatma yöntemleri (sosyal mühendislik) ve veri sızıntısı gibi çeşitli dijital saldırı tekniklerinden faydalanmaktadır. Veri sızıntıları ve ihlalleri, erişim hakları bulunmayan kişiler tarafından özel içeriklerin ele geçirilmesi ya da yayımlanması durumlarını kapsar ve ciddi güvenlik açıklarına yol açma potansiyeli taşır [2, 3].

Siber saldırılar istatistiksel olarak incelendiğinde 2010 yılından itibaren fidye yazılımları, saldırganlar için önemli bir gelir kaynağı haline gelmiş, 2017 yılı sonunda fidye yazılımı vakalarında önceki yıllara kıyasla 3 katı aşkın bir yükseliş yaşanmıştır. 2017 sonunda dünya genelindeki şirketlerin her 40 saniyede bir saldırıya uğradığı tespit edilmiş ve yaklaşık 10 saldırından 6'sının fidye saldırısı olduğu saptanmıştır. Bu saldırılardan şirketlerin %72'si etkilenmiş ve maddi zararı 2017 sonlarında küresel düzeyde yaklaşık 5 milyar dolar civarındadır [4]. 2022 yılında ise küresel anlamda sadece kamu kurum ve kuruluşlarına yönelik saldırılar 40.000 dolaylarında iken 2023 yılında bu sayı yaklaşık olarak 100.000 olarak saptanmıştır [5]. AB Siber Güvenlik Ajansı (ENISA) 2024 verilerine göre saldırıların yaklaşık %27'si fidye yazılımı kapsamında değerlendirilmiştir [6]. İstatistiklerin gösterdiği tüm bu sorunlardan hareketle yapılan çalışmada siber saldırılar özelinde fidye yazılımlarında anomalileri ve sahte imzaları tespit etmek hedeflenmiş, ilgili sorunun çözümü için literatüre katkı sağlanmıştır. Geleneksel çözümler hem hız hem de doğruluk açısından siber saldırıları tespit etmek için yetersiz kalabilmektedir. Bu alanda daha etkili, yenilikçi, çağın gereksinimlerine uygun, uyarlanabilir yaklaşımlara ihtiyaç vardır. İstatistiksel olarak ekonomik kayıplar, şirketlerin veri sızıntıları, kamu kurum ve kuruluşlarına gerçekleştirilen saldırıların etki sahası düşünüldüğünde yapay zekâ tabanlı çözümlerin siber güvenlik stratejilerinin ayrılmaz bir parçası olarak ortaya çıkmış olduğu görülmektedir [3]. Son dönemlerde klasik yaklaşımlar yerine derin öğrenme tabanlı yaklaşımlar dikkat çekmektedir. Bu çalışma derin öğrenme yaklaşımlarından hareketle 1B sinyal verilerini 2B görsellere dönüştürerek, ilgili görselleri siber saldırı tespitinde kullanması ve ilgili problemlere çözüm sunması açısından önemlidir.

Bu çalışmada kullanılan veri seti Kaggle platformunda açık erişimli olarak sunulmuştur. Veri seti, zaman-frekans serisi verilerini görsele dönüştüren yöntemler kullanılarak ön işleme adımlarından geçirilmiş ve derin öğrenme tabanlı ViT model ile analiz edilmiştir. Başarı oranı düşük yöntemler elenirken, dalgacık dönüşümler ile elde edilen veriler üzerinde hem özellik seçimi hem de makine öğrenmesi yöntemi sınıflandırma aşamasında uygulanmıştır. Sonuçlar çapraz doğrulama ile teyit edilmiştir. Elde edilen yüksek doğruluk sonucuyla, görsel tabanlı derin öğrenme yaklaşımlarının fidye yazılımlarında anomali ve sahte imza tespitinde güçlü bir çözüm sunabileceği gösterilmektedir. Bu çalışmanın amacı fidye yazılımlarında anomali ve sahte imzaların derin öğrenme yöntemlerinden ViT model ile örüntülerinin ayırt edilmesi ve sınıflandırılmasının tespitine yöneliktir.

Bu çalışma, geleneksel yöntemlerin aksine yapay zekâyı siber saldırı tespitinde kullanarak, derin öğrenme yöntemlerinin fidye yazılımlarında anomalileri ve sahte imzaları belirlemedeki etkisini tespit etmeyi hedeflemiş ve aşağıdaki maddelerle literatürdeki boşlukları doldurarak katkı sunmuştur:

- Fidye yazılımlarının tespiti için literatürdeki sınırlı ve tek boyutlu öznitelik çıkarımı yöntemlerinin ötesine geçerek zaman-frekans dönüşümlerine dayalı spektral görüntüleme ve derin öğrenme tekniklerini entegre eden özgün bir yaklaşım sunmaktadır.
- CMT, CWT, FCWT ve Kalman filtresi dönüşümleri aracılığıyla elde edilen 2B görüntüleriyle zaman-frekansa bağlı desenler yakalanmış, bu da geleneksel yöntemlerin sunduğu doğruluk oranlarının üstünde performans sergilemektedir.
- Önerilen yaklaşımda özellik seçim yöntemleri kullanılarak verimli özelliklerin seçimi gerçekleştirilmiş ve böylece donanım-zaman maliyetleri düşürülmüştür.
- Çalışmada kullanılan veri seti test edilerek yalnızca teorik değil aynı zamanda pratik açıdan da güçlü bir katkı sunmuş böylece gerçek dünya senaryolarına uygulanabilirliği yüksek, ölçeklenebilir ve genellenebilir model önerisi oluşturulmuştur.

Bu makalenin diğer bölümleri şu şekilde yapılandırılmıştır: 2. Bölümde detaylı literatür incelemesi yapılmış ve çalışmanın ayrılan yönleri ele alınmıştır. 3. Bölümde veri kümesi hakkında ayrıntılı bilgiyle beraber görüntü işleme yöntemleri, yapay zekâ yaklaşımları ve önerilen model detaylandırılmaktadır. 4. bölümde, bulgular, deneysel analizler ve yapılan yorumlar yer almaktadır. Sonraki bölümlerde ise tartışma ve sonuç kısmı ele alınmaktadır.

2. Literatür İncelemesi

Dijitalleşme ile birlikte siber saldırılar, fidye yazılımları gibi zararlı yazılımlar; bireyler, şirketler, kamu kurum ve kuruluşları ve devletler için ciddi bir tehdit haline gelmiştir. Bu tür yazılımlar genellikle sistemlere sızarak verileri şifrelemekte ve kullanıcıların erişimini engelleyerek hem veri gizliliğini hem de bütünlüğünü tehdit etmektedir. Geleneksel siber güvenlik yöntemlerinin bu saldırıların tespitinde yetersiz kalması, daha hızlı, doğru ve etkili analiz yaklaşımlarına olan ihtiyacı artırmaktadır. Bu bilgilerden hareketle literatür incelendiğinde çeşitli çalışmaların yapıldığı görülmüştür.

Zahra ve ark. [7] çalışmasında anomali tabanlı saldırı tespit sistemlerinin etkinliğini artırmak amacıyla destek vektör makineleri (SVM), karar ağaçları (DT), naif bayes (NB), ve topluluk öğrenmesi gibi makine öğrenmesi yaklaşımlarını kullanmışlardır. Optimizasyon yöntemleriyle sonuçları artırmayı hedefleyerek alana katkı sunmuşlardır. Toğaçar [8] çalışmasında ağ teknolojisi verilerinde siber saldırıları tespit etmeyi amaçlamış ve arşimet optimizasyon algoritmalarını kullanmıştır. Softmax sınıflandırıcı kullanılan çalışmada trafo tabanlı evrişimsel sinir ağı (CNN) modeliyle ilgili veriler eğitilerek test edilmiş ve %98.94 oranında doğruluk performansı elde etmiştir. Torky [9] yaptığı çalışmada veri setindeki düzensizlikleri ve anomalileri tespit etmek için en yakın komşu (KNN), SVM, açısal tabanlı aykırı değer tespiti (ABOD) algoritmalarını kullanarak analiz yapmıştır. En yüksek sonucu %80.2 ile SVM yaklaşımıyla elde etmiştir. Igugu [10] çalışmasında bulut ortamlarındaki siber saldırıları tespit etmeyi amaçlamış ve makine öğrenmesi algoritmaları kullanmıştır. Çalışma kendi içinde %99 gibi bir sonuç verse de gerçek dünya verilerinde yapılan testlerle makine öğrenmesi algoritmalarının doğruluk oranında düşüş yaşandığı tespit edilmiştir. Yan ve ark. [11] yaptıkları çalışmada fidye yazılımlarında anomali tespiti için makine öğrenmesi algoritmaları kullanmıştır. İki katmanlı bir sistem kullanılan çalışmanın ilk katmanda topluluk öğrenmesi (Ensemble) modeli kullanılmış ve %98.2 doğruluk elde edilmiştir. İkinci katmanında LightGBM kullanılarak fidye yazılımlarındaki anomaliler sınıflandırılmış %74.9 ile %99.1 arasında değişen doğruluk oranlarıyla önemli bulgular sunmuştur. Por ve ark. [12] yaptıkları çalışmada siber saldırılarda anomali tespitine yoğunlaşan 1132 çalışmayı incelemiş ve bu çalışmalardan 53 nitelikli çalışma ayrıca analiz edilmiştir. Çalışmada değerlendirilen yöntemler arasında makine öğrenmesi, derin öğrenme, anomali tespiti yaklaşımları ve hibrit modeller öne çıkmaktadır. Çalışma, YZ tabanlı çözümlerin siber güvenlik bağlamında yüksek potansiyele sahip olduğunu ortaya koyarken, gelecekteki çalışmalar için daha sağlam, ölçeklenebilir ve dinamik yapay zekâ modellerinin geliştirilmesine ihtiyaç olduğunu vurgulamıştır. Derin öğrenme tabanlı yaklaşımların yüksek hesaplama gücü ve zaman gereksinimlerine rağmen siber saldırılardaki anomalilerin karmaşık kalıpları tespit etmede umut verici olduğunu ifade etmiştir. Kumar ve ark. [13] çalışmamızda kullanılan veri setiyle yaptıkları çalışmada fidye yazılımlarının

ciddi bir güvenlik tehdidi haline geldiğini ifade etmiştir. Fidye yazılımlarındaki anomalileri tespit etmek amacıyla AdaBoost, RF, NB, K-NN, SVM, LR, NN gibi yaklaşımlar kullanılmıştır. En yüksek sonuç %92.2 doğruluk oranıyla topluluk öğrenmesi modelinde tespit edilmiştir. Alzahrani ve ark. [14] yaptıkları çalışmada transformer tabanlı RansomFormer modelini tanıtarak çeşitli veri setleri üzerinde testler gerçekleştirmiş ve %99 ile %99.5 arasında doğruluk oranı tespit edilmiştir. Mohamed ve ark. [15] yaptıkları çalışmada siber saldırı tespiti için kendilerinin tasarladığı yaklaşım ile yenilikçi hibrit model önermiş ve %98-%99 aralığında doğruluk oranları sağlamıştır. Son yıllarda siber güvenlik alanında sinyal-görüntü dönüşüm yaklaşımları, ağ trafiği ve davranışsal verilerdeki lokal ve çok ölçekli örüntülerin ortaya çıkarılmasında etkili bir yöntem olarak öne çıkmaktadır. Zaman-frekans temsilleri üzerinden oluşturulan spektral görüntülerin derin öğrenme ve transformer tabanlı modellerle analiz edildiği güncel çalışmalar mevcuttur. Yapılan çalışmalar bu yaklaşımların geleneksel istatistiksel yöntemlere kıyasla daha yüksek ayırt edicilik sunduğunu göstermektedir [16,17]. Bununla birlikte, literatürde ağ trafiği ve zaman-frekans temsillerine dayalı çalışmalarda CNN mimarileri sıklıkla tercih edilmiştir. Ancak CNN tabanlı yaklaşımlar, yerel alıcı alanlara dayalı yapıları nedeniyle spektral görüntülerdeki küresel örüntüleri sınırlı ölçüde modelleyebilmektedir. ViT mimarisi ise, CNN tabanlı yaklaşımlardan farklı olarak, küresel bağlamı kendi kendine dikkat mekanizmasıyla doğrudan modelleyebilmekte ve görüntü içerisindeki uzun menzilli bağımlılıkları etkili biçimde öğrenebilmektedir. Bu özellik, zaman-frekans temsillerinde ortaya çıkan çok ölçekli ve dağınık saldırı örüntülerinin yakalanması açısından ViT modelini uygun bir aday hâline getirmektedir. Zaman-frekans temsilleri üzerinden elde edilen spektral görüntülerde saldırı örüntülerinin yalnızca lokal özelliklerle değil, farklı ölçekler arasındaki ilişkilerle de tanımlandığı bilinmektedir. Bu tür çok ölçekli ve küresel bağımlılıkların modellenmesi açısından, kendi kendine dikkat mekanizmasına dayalı transformer tabanlı yaklaşımların yapısal bir avantaj sunduğu değerlendirilmektedir. Nitekim literatürde, siber güvenlik ve anomali tespiti problemlerinde transformer tabanlı modellerin, görüntü içerisindeki uzun menzilli ilişkileri daha etkin biçimde temsil edebildiği tespit edilmiştir. Bu yönüyle CNN tabanlı mimarilere tamamlayıcı veya alternatif bir çözüm sunduğu rapor edilmektedir [18].

Siber saldırı tehditlerinin artış gösterdiği günümüzde geleneksel yöntemler karmaşık ve çok boyutlu siber saldırılarla başa çıkmakta yetersiz kalabilmektedir. Literatürdeki statik analiz yaklaşımları genellikle dosya yapısı, imza veya tekil API çağrısı gibi sınırlı özniteliklere dayanır ve yetersiz kalmaktadır [14]. Yapılan çalışma özellikle statik analizlere veya klasik makine öğrenmesi yöntemlerine dayanan yaklaşımlara göre daha güçlü ve uygulanabilir bir çözüm ortaya koymaktadır. Yapılan çalışma, hem kullanılan yöntemler hem de elde edilen sonuçlar incelendiğinde diğer çalışmalardan ayrılarak, fidye yazılımlarında anomali ve sahte imza tespitine yönelik olarak literatüre anlamlı katkılar sunmaktadır.

3. Materyal ve Metod

Bu bölümde ilgili veri seti tanıtılmış, ön işlem yöntemleri, önerilen model ve modelin değerlendirme kriterlerine detaylı bir şekilde yer verilmiştir.

3.1. Veri Seti

Çalışmada kullanılan veri seti Kaggle platformunda herkese açık bir şekilde erişime sunulmuştur. Veri setinde saldırı zamanlarının izlenmesini sağlayan zaman damgaları, saldırı türlerinin sınıflandırılmasına yönelik bayraklar, saldırı yöntemlerinin anlaşılmasına yardımcı olan protokol verileri, veri aktarım eğilimlerini incelemek için ağ akış bilgileri ve fidye yazılımı sınıflandırmaları gibi birçok kritik bilgi yer almaktadır. Ayrıca veri seti hem USD hem de Bitcoin (BTC) cinsinden finansal zararı ölçmekte, ilgili kötü amaçlı yazılımlar hakkında bilgi sunmakta ve örüntü tanıma süreçlerinde sayısal kümeleme yöntemlerini kullanmaktadır. Veri setinde her bir veri noktası belirli bir değeri ve buna bağlı olarak bir etiket (“S”, “SS” ve “A”) içermektedir. Bu veri setinde S: “İmza”, SS: “Sahte İmza”, A: “Anomali” olarak etiketlenmiştir. Veri seti fidye yazılımlarında sahte imza ve anomalileri tespit etmek için kullanılmıştır. Orijinal veri seti 207.553 satır ve 14 sütundan oluşan CSV uzantılı dosya formatıdır. 14 sütunda yer alan veriler, veri setinin

parametrelerini ve parametrelere ait değerlerini oluşturmaktadır [19]. Bu bilgiler Çizelge 1'de özetlenmiştir ve özniteliklere ait detaylar Çizelge 2'de açıklanmıştır.

Çizelge 1. Veri setinin öznitelikleri ve biçimleri.

Sütun	Öznitelik	Örnek	Biçim
1	Zaman (Time)	50	Sayısal
2	Protokol (Protcol)	TKP	Kategorik
3	Bayrak (Flag)	A	Kategorik
4	Aile (Family)	WannaCry	Kategorik
5	Kümeler (Clusters)	1	Sayısal
6	Güvenli Adres (SeddAddress)	1DA11mPS	Kategorik
7	Açıklanan Adres (ExpAddress)	1BonuSr7	Kategorik
8	Bitcoin (BTC)	1	Sayısal
9	Amerikan Doları (USD)	500	Sayısal
10	Ağ Trafiği (Netflow_Bytes)	5	Sayısal
11	IP Adresi (IPaddress)	A Sınıfı	Kategorik
12	Tehditler (Threats)	Bone	Kategorik
13	Liman (Port)	5061	Sayısal
14	Tahmin (Prediction)	SS	Kategorik

Çizelge 2. Veri setinin öznitelik açıklamaları.

Sütun	Öznitelik	Açıklaması
1	Zaman	Ağ saldırılarının zaman damgasını gösteren nicel sütun
2	Protokol	Kullanılan ağ protokolünü temsil eden nitel/kategorik sütun
3	Bayrak	Ağ bağlantı durumunu gösteren nitel/kategorik sütun
4	Aile	Ağ ihlali kategorisini tanımlayan nitel/kategorik sütun
5	Kümeler	Olay kümelerini veya gruplarını belirten tamsayılara sahip sütun
6	Güvenli Adres	Biçimlendirilmiş fidye saldırıları bağlantılarını temsil eden sütun
7	Açıklanan Adres	Orijinal fidye saldırı bağlantılarını gösteren sütun
8	Bitcoin	Saldırılardaki Bitcoin işlemleriyle ilgili değerlerin bulunduğu sütun
9	Amerikan Doları	Saldırıların neden olduğu mali zararları gösteren sayısal sütun
10	Ağ Trafiği	Ağ akışında aktarılan baytları gösteren sütun
11	IP Adresi	Ağ olaylarıyla ilişkili IP adreslerini içeren sütun
12	Tehditler	Tehditlerin veya saldırıların niteliğini temsil eden sütun
13	Liman	Olaylarda ağ bağlantı noktası numarasını gösteren sütun
14	Tahmin	Tahmini model sonuçlarını gösteren hedef değişken (Anomali (A), İmza (S) ve Sentetik İmza (SS))

Bu çalışmada veri setinin tüm kayıtları kullanılmamıştır. Her bir sınıftan rastgele seçilen 1000'er veri kaydıyla önerilen yaklaşım eğitilmiştir. Burada amaç önerilen modelin zaman ve donanım maliyetini düşürmektir. Çalışmada kullanılan ViT mimarisi, sıfırdan eğitilen bir model olarak değil, büyük ölçekli görsel veri kümeleri üzerinde önceden eğitilmiş bir temsil öğrenme modeli olarak kullanılmıştır. ViT mimarisinin geniş ölçekli veri kümeleri üzerinde ön eğitimden geçirilmesi durumunda, aktarım öğrenimi yoluyla farklı görevlerde etkili ve genellenebilir temsiller üretebildiği literatürde raporlanmıştır. Güncel çalışmalar, önceden eğitilmiş transformer tabanlı görsel modellerin özellikle sınırlı ancak dengeli veri kümelerinde daha kararlı sonuçlar verdiğini göstermiştir. Bu modellerin çoğu uygulamada derin özellik çıkarıcı olarak kullanılmasının uygun bir yaklaşım olduğunu vurgulamaktadır [18,20]. Bu doğrultuda ViT modeli, çalışmamızda yüksek parametreli bir uçtan uca sınıflandırıcıdan ziyade, zaman-frekans temsillerinden ayırt edici özellikler çıkaran bir derin özellik çıkarıcı bileşen olarak konumlandırılmıştır. Çalışmada kullanılan veri setinde 200.000'in üzerinde kayıt bulunmasına rağmen, deneylerde her sınıftan eşit sayıda örnek seçilerek dengeli bir alt veri kümesi oluşturulmuştur. Bu tercih yalnızca hesaplama maliyetlerini azaltmak amacıyla değildir. Sınıf dengesizliğinin öğrenme sürecinde oluşturabileceği yanlılığı önlemek ve özellikle sahte imza gibi kritik sınıfların adil biçimde temsil edilmesini sağlamak amacıyla yapılmıştır. Sınıf dengesizliğinin sınıflandırma performansını olumsuz etkilediği ve dengeli

örnekleme stratejilerinin model genellenebilirliğini artırdığı gösterilmiştir [21,22]. Bununla birlikte, tüm veri seti üzerinde kapsamlı eğitim ve test yapılmasının yüksek hesaplama maliyeti gerektirdiği dikkate alınarak, bu durum çalışmanın bir sınırlılığı olarak ele alınmıştır. Veri seti ve eğitiminin istatistiksel bilgileri Çizelge 3'de verilmiştir.

Çizelge 3. Veri seti istatistiği.

	Etiketler		
	A (Anomali)	S (İmza)	SS (Sahte İmza)
Rastgele Seçilen Değer	1000	1000	1000
Eğitim Verisi (%70)	700	700	700
Test Verisi (%30)	300	300	300
Orijinal Veri Sayısı	24437	46414	33777

Fidye yazılımlarında anomali ve sahte imza tespiti için CSV uzantılı veri seti üzerinde ön işlemler uygulanmıştır. Yapılan işlemle 1B numerik veriler CMT, CWT, FCWT ve Kalman filtre tabanlı görüntüleme yöntemleriyle 2B görsel verilere dönüştürülmüştür.

3.2. Sürekli Dalgacık Dönüşümü

Sürekli dalga dönüşümü (CWT), zaman-frekans çözünürlüğü sağlayarak ani değişimleri başarılı şekilde yakalamaya olanak tanır. CWT, sinyalin farklı frekans bileşenlerini zaman ekseninde lokalize ederek analiz eder. Bu yöntem, özellikle ani geçişlerin ve geçici olayların tespitinde etkilidir ve yüksek zaman-frekans çözünürlüğü sunar. CWT bir zaman serisinin zaman-frekans (TF) düzlemindeki yapısal özelliklerini ortaya koymak ve analiz etmek amacıyla kullanılır [23].

CWT matematiksel olarak Denklem 1'de gösterilen formül aracılığıyla hesaplanmaktadır. Bu formülde analiz edilen sinyal $\mathbf{x(t)}$, dalga fonksiyonu $\boldsymbol{\psi}$, sıkıştırma katsayısı "$\boldsymbol{a}$" ve kaydırma katsayısı "$\boldsymbol{b}$" ile ifade edilmektedir.

$$\mathrm{CWT} + (a, b) = \int_{-\infty}^{\infty} x(t) \cdot \psi * \left(\frac{t - b}{a}\right) dt \quad (1)$$

3.3. Hızlı Sürekli Dalgacık Dönüşümü

Hızlı sürekli dalga dönüşümü (FCWT)'nün daha hızlı hesaplanan versiyonudur ve büyük veri setlerinde verimlidir. FCWT, geleneksel CWT dönüşümüne kıyasla daha düşük hesaplama maliyeti ile benzer zaman-frekans analizini gerçekleştirebilen bir dönüşümdür. Büyük veri kümelerinde uygulanabilirliği ve işlem verimliliği ile öne çıkar [24]. CWT'nin sağladığı yüksek zaman-frekans çözünürlüğünü koruyarak işlem süresini önemli ölçüde azaltan FCWT, özellikle yüksek hacimli verilerin analizinde önemli bir avantaj sunmaktadır. Bu dönüşüm yöntemi; elektroensefalografi (EEG), elektromiyografi (EMG) gibi biyomedikal sinyallerin çözümlenmesi, siber güvenlik alanında anomali tespiti ve mekanik sistemlerde titreşim analizleri gibi çeşitli gerçek zamanlı uygulamalarda etkili bir araç olarak öne çıkmaktadır. FCWT, klasik CWT'nin zaman alanındaki hesaplamaları yerine frekans alanında işlem yapan Fourier dönüşümüne dayalı bir yapıya sahiptir. Bu yöntemde Morlet gibi karmaşık dalgacık fonksiyonları kullanılarak sinyalin farklı frekans ölçeklerine karşılık gelen spektral bileşenleri yüksek hızda elde edilebilmektedir.

FCWT algoritmasının temel işlem adımları şu şekilde sıralanabilir:

1. Giriş sinyali, Hızlı Fourier Dönüşümü (FFT) kullanılarak frekans alanına aktarılır.
2. Her bir dalgacık ölçeği için frekans alanında sinyal ile dalgacık fonksiyonu arasında çarpım işlemi gerçekleştirilir.

3. Frekans alanında elde edilen bu ara sonuçlar, Ters Hızlı Fourier Dönüşümü (IFFT) ile yeniden zaman alanına dönüştürülerek dalgacık katsayıları elde edilir.

FCWT, klasik CWT'ye kıyasla yaklaşık 100 kat daha hızlı çalışabilmekte ve %98'in üzerinde yapısal benzerlik sağlayarak doğrulukta kayda değer bir azalma yaşanmadan yüksek verimlilik sunmaktadır [25].

3.4. Karmaşık Morlet Dönüşümü

Karmaşık morlet dönüşümü (CMT), CWT'nin özel bir versiyonudur. Morlet dalgacığı kullanarak spektral bileşenlerin zaman içindeki değişimini hassas biçimde analiz eder. Bu özellik, özellikle saldırı örüntülerinin zamana yayılmış analizinde faydalıdır [26]. CMT, sinyallerin hem zaman hem de frekans bileşenlerinin ayrıntılı şekilde incelenmesine olanak tanıyan gelişmiş bir analiz tekniğidir. Bu yöntem, dalgacık tabanlı analiz yaklaşımlarından biri olup, belirli bir sinüs dalgasının Gauss penceresiyle çarpılması sonucu elde edilen özgün bir dalga formuna dayanır [27]. Özellikle biyomedikal alanlarda, örneğin beyin dalgalarının incelenmesi ve EEG sinyallerinin yüksek çözünürlüklü frekans analizi gibi uygulamalarda yaygın olarak kullanılmaktadır.

CMT yönteminin matematiksel olarak gösterimi Denklem 2'de verilmiştir. Bu denklemde genlik olarak $\boldsymbol{A}$ değişkeni kullanılmıştır. Zaman ekseninde sınırlı bir pencereleme etkisi yaratan Gauss fonksiyonunu ifade eden işlem $\mathbf{exp}\left(-\frac{\mathbf{t^2}}{\mathbf{2\sigma^2}}\right)$ olarak gösterilmiştir. $\mathbf{cos(2\pi f_0 t)}$ işlemi ise sinyaldeki frekans bileşenlerini modelleyen sinüs fonksiyonuna karşılık gelmektedir. $\boldsymbol{f_0}$ parametresi frekans bilgisini taşırken, $\boldsymbol{\sigma}$ ise Gauss fonksiyonunun bant genişliğini belirleyen değişken olarak tanımlanmaktadır.

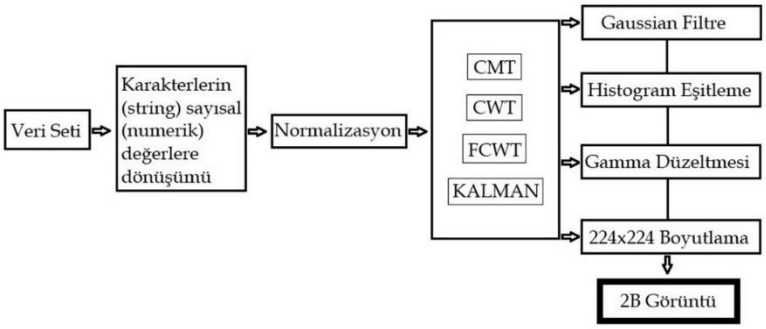
$$\psi(t) = A \cdot \exp\left(-\frac{t^2}{2\sigma^2}\right) \cdot \cos(2\pi f_0 t) \tag{2}$$

3.5. Kalman Filtresi

Kalman filtresi, zamana bağlı sistemlerde gürültüleri filtrelemek ve değerleri tahmin etmek amacıyla kullanılan doğrusal bir kestirim algoritmasıdır. Özellikle saldırı akışlarında sezgisel gürültü azaltımı için kullanılmıştır [28]. Bununla birlikte Kalman filtresi doğrusal dinamik modellerdeki sistem durumunu geçmiş gözlemler ve model parametreleri kullanarak yinelemeli biçimde tahmin eden bir kestirim tekniği olarak ifade edilir [29]. Kalman filtresinin durum matrislerinden arındırılmış [30] matematiksel gösterimi Denklem 3'de gösterilmiştir. $\widehat{\boldsymbol{X}}_{\boldsymbol{k}}$ parametresi sinyal tahmin değerini, $\boldsymbol{k}$ değişkeni evreleri (states), $\boldsymbol{Z_k}$ parametresi ölçülen değeri, $\boldsymbol{K_k}$ kalman kazancı değerini, $\widehat{\boldsymbol{X}}_{\boldsymbol{k-1}}$ işlemi ise sinyalden önceki durumu ifade eden parametredir.

$$\hat{X}_k = K_k \cdot Z_k + (1 - K_k) \cdot \hat{X}_{k-1} \tag{3}$$

Bu çalışmanın deneysel analizlerinde kullanılan önişlem yöntemlerinin iş boru hattı Şekil 1'de gösterilmiştir.



Şekil 1. Görüntüleri oluşturmak için yapılan ön işlemler.

3.6. Görüntü Dönüştürücü

Görüntü Dönüştürücü (ViT), klasik görüntü sınıflandırma görevlerinde görüntüleri doğrudan dönüştürücü (transformer) mimarilerine uygulayan bir yöntemdir. Geleneksel yaklaşımların aksine ViT, bir görüntüyü sabit boyutlu parçalara bölerek bu parçaları bir dizi (sequence) hâline getirir. ViT, doğal dil işleme (NLP) alanında yaygın olarak kullanılan transformer yapısını doğrudan görsel verilere uygular [31]. Model giriş verilerinin her bir bileşenine farklı ağırlıklar atayarak önemini belirleyen ve kendi kendine dikkat (self attention) mekanizmasına dayanan bir derin öğrenme mimarisidir. Başlangıçta doğal dil işleme ve bilgisayarla görme alanlarında kullanılmak üzere geliştirilmiştir. Transformer modelleri, çeviri ve metin özetleme gibi görevlerde, doğal dildeki sıralı verileri işlemek amacıyla tasarlanmışlardır [32]. Bununla birlikte, bu modeller verileri zorunlu olarak sıralı biçimde işlemezler. Dikkat mekanizması sayesinde, giriş dizisinin herhangi bir konumundaki öğe için bağlamsal bilgi sunabilir.

ViT modeli görüntü verilerini analiz etmek için çok aşamalı bir mimariye sahiptir. İlk aşamada, giriş gömüleme katmanı aracılığıyla görüntüler belirli çözünürlüklerdeki yamalara ayrılır. İkinci aşamada, her bir yama vektör temsiline dönüştürülerek modelin işleyebileceği bir forma getirilir. Üçüncü aşamada, konum gömülemeleri eklenerek yamaların sıralaması ve konumsal bilgileri modele tanıtılır. Dördüncü aşamada, Çoklu Başlı Kendine Dikkat (MHSA) ve İleri Beslemeli Sinir Ağı (FFNN) bileşenlerinden oluşan birden fazla Transformer kodlayıcı bloğu yer alır. Bu bloklar, yamalar arası ilişkileri modelleyerek ve özellik çıkarımı yaparak derin öğrenme sürecini destekler. Beşinci aşamada, kodlayıcı bloklar yığılarak daha karmaşık ve derin özelliklerin öğrenilmesi sağlanır. Son aşamada ise çıkış katmanı bulunur ve bu katman genellikle sınıflandırma görevlerinde kullanılır. Bu aşamada softmax gibi aktivasyon fonksiyonları tercih edilebilir [33,34]. ViT modelinde, giriş görüntüleri sabit boyuttaki küçük yamalara ayrılarak birer indeks dizisi şeklinde işlenir [35]. Şekil 2'de transformer model akış şeması gösterilmiştir.

Denklem 4'de giriş görüntüsünden elde edilen toplam $\boldsymbol{P}$ boyutundaki yama sayısını ifade etmektedir. $\boldsymbol{H}$ parametresi görüntünün yüksekliğini $\boldsymbol{W}$ ise genişliğini ifade etmektedir.

$$N = \frac{HxW}{p^2} \tag{4}$$

Denklem 5'de $\boldsymbol{E}$, öğrenilebilir bir gömüleme matrisi olarak tanımlanırken, $\boldsymbol{z_0^i}$ ifadesi $\boldsymbol{i}$'inci yamanın gömülenmiş (embedded) vektörünü ve $\boldsymbol{e_{pos}^i}$ ifadesi ise ilgili yamanın pozisyonel kodlamasını temsil etmektedir.

$$z_0^i = E.x_i + e_{pos}^i, for\ i = 1, \dots, N \tag{5}$$

Denklem 6'da $\boldsymbol{Q}$; sorgu (query), $\boldsymbol{K}$; anahtar (key) ve $\boldsymbol{Z}$; değer (value) matrislerini temsil etmektedir. $\boldsymbol{d_k}$ ise başlık (head) boyutunu ifade eder.

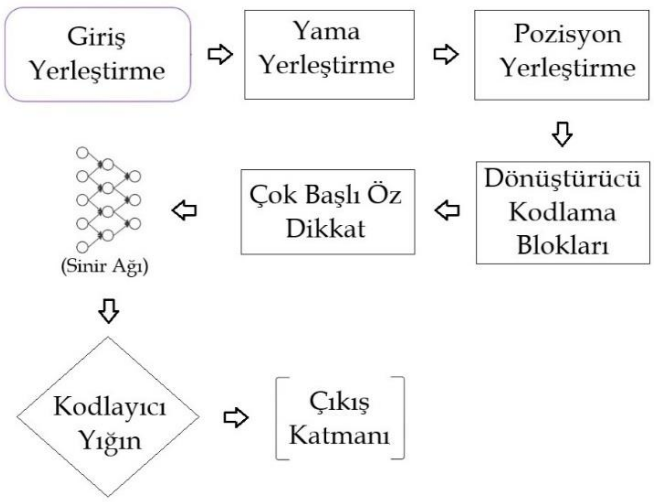
$$Attention\ (Q, K, V) = softmax(\frac{QK^T}{\sqrt{d_k}})V \tag{6}$$

Denklem 7'de $\boldsymbol{MLP}$, ileri beslemeli bir yapay sinir ağını ifade eder. $\boldsymbol{z_l}$ ifadesi $\boldsymbol{l}$'inci katmandan gelen giriş vektörünü temsil etmektedir.

$$z_{l+1} = MLP\big(Attention(zl)\big) + zl \tag{7}$$

Denklem 8'de $\boldsymbol{w_{fc}}$, sınıflandırma amacıyla kullanılan ağırlık matrisi olarak tanımlanmakta olup, $\boldsymbol{z_l}$ ifadesi ise son Encoder katmanından elde edilen çıktı vektörünü göstermektedir.

$$\hat{y} = softmax(w_{fc}.z_l) \tag{8}$$



Şekil 2. Dönüştürücü (Transformatör) modellerin genel iş boru hattı.

3.7. Özellik Seçim Yöntemleri: mRMR-Relief

En az yineleme en fazla ilgililik (mRMR) algoritması, giriş verilerinden elde edilen özellik kümelerini işleyerek en uygun özellikleri seçmeyi amaçlayan bir filtreleme yöntemidir. Özellikle ikili sınıflandırma problemlerinde başarılı sonuçlar vermektedir. Algoritma, özellikleri temsil eden sayıları kullanarak bu özellikler arasındaki ilişkiyi belirlemeye çalışır ve bu ilişkiyi bir puan ile değerlendirir. Daha yüksek puan alan özellikler, daha güçlü bir ilişkiye sahip olarak kabul edilir. Bu yaklaşım sayesinde mRMR, en zayıf özellikleri artık (residual) özellikler, en güçlü özellikleri ise uygun (relevant) özellikler olarak sınıflandırır. mRMR yöntemi temel olarak özellikler arasındaki benzerlik ve ilişkileri analiz etmeye odaklanır [36,37].

$$Maksimize = \frac{V}{W} \tag{9}$$

Denklem 9'da maksimum ilgililik (W) ve minimum gereksizlik (V) değerleri mRMR algoritmasıyla hesaplanır. $\boldsymbol{V}$ genellikle özelliklerin hedef değişkenle olan ilişkisini temsil eder. Bu, her bir özelliğin hedef değişkenle olan karşılıklı bilgisini (mutual information) ölçer ve maksimum ilgililiği ifade eder. $\boldsymbol{W}$ ise seçilen özellikler arasındaki benzerliği veya korelasyonu ölçer. Bu durum, modelin karmaşıklığını artırabilir veya aşırı öğrenme (overfitting) riskini yükseltebilir. Bu nedenle, $\boldsymbol{V}$ değeri seçilen özellikler arasındaki gereksiz benzerliklerin en aza indirilmesi gerektiğini ifade eder. Yüksek ilgililik ve düşük gereksizlik arayışını birleştirir ve max fonksiyonu, bu oranı en üst düzeye çıkaran özelliklerin seçilmesini hedefler. Sonuç olarak, bir puan tablosu oluşturulur, her bir özelliğin puanı hesaplanır ve özellik puanları arasında bir sıralama yapılır.

Relief yöntemi, yüksek boyutlu özellik uzayında en verimli özelliklerin belirlenmesini amaçlayan ve özellikler arasındaki en yakın komşu hesaplamalarına dayalı bir yaklaşım sunan bir yöntemdir. Bu yöntemde, özellik seçimi sürecinde en yakın komşu sayısı rastlantısal bir algoritma aracılığıyla belirlenmekte; aynı şekilde, rastgele seçilen özellikler eşik değerlerinin tespitinde de kullanılmaktadır. Söz konusu durum, performans maliyeti gibi çeşitli avantajlara veya dezavantajlara yol açabilmektedir. Relief yöntemi, tek değişkenli (univariate) yöntemlere benzer şekilde her bir özelliği ayrı ayrı sıralamaktadır. Sonrasında ise sıralanan tüm özellikler arasındaki bağımlılıkları çok değişkenli (multivariate) bir yaklaşımla değerlendirerek daha nesnel bir analiz sağlamaktadır. Örneğin, özellikler kümesinde her bir özellik için en yakın komşular belirlenmekte ve her bir özellik için hiperboyutlu bir karar sınırı hesaplanmaktadır. Bu yöntemin temel amacı, hedef özelliğin belirlenmesidir. Hedef özelliğin skoru, karar sınırına yakın konumlanan komşu özellik değerleri doğrultusunda güncellenmektedir. Bu yaklaşım, Relief yönteminin benzerlik ve farklılıkları daha etkin biçimde hesaplayabilmesini mümkün kılmaktadır [38,39].

3.8. Naif Bayes

NB, özellikler arasında bağımsızlık varsayımına dayanarak olasılık teorisini kullanan bir sınıflandırma algoritmasıdır [40]. Söz konusu varsayıma rağmen, özellikler arasında güçlü bir ilişki bulunmadığı durumlarda oldukça etkili sonuçlar verebilmektedir. Algoritma, bir veri örneğinin belirli bir sınıfa ait olma olasılığını, her bir özelliğin ilgili sınıfta bağımsız olarak ortaya çıkma olasılıklarına dayanarak hesaplamaktadır [41]. NB sınıflandırma yöntemi, temelini Bayes teoreminden almakta ve bu teoremin olasılıksal çıkarım gücüne dayalı bir yaklaşım sunmaktadır.

Denklem 10'da $\boldsymbol{P(C_k \backslash x)}$, belirli bir $\boldsymbol{x}$ veri noktası göz önüne alındığında, bu noktanın $\boldsymbol{C_k}$ sınıfına ait olma olasılığını belirtir. $\boldsymbol{P(x \backslash C_k)}$, $\boldsymbol{C_k}$sınıfına ait olduğu bilinen bir durumda, $\boldsymbol{x}$ veri noktasının gözlenme olasılığını ifade eder. $\boldsymbol{P(C_k)}$, $\boldsymbol{C_k}$ sınıfının önsel (prior) olasılığını, $\boldsymbol{P(x)}$ ise $\boldsymbol{x}$ veri noktasının toplam (marjinal) olasılığını temsil etmektedir. NB yaklaşımında modelin temel varsayımı, özelliklerin (öz niteliklerin) birbirinden bağımsız olduğudur.

$$P(C_k \backslash x) = \frac{P(x \backslash C_k) P(C_k)}{P(x)} \tag{10}$$

Denklem 11'de $\boldsymbol{x_i}$ ifadesi, $\boldsymbol{x}$ veri noktasının $\boldsymbol{i'}$inci öz niteliğine karşılık gelmektedir. NB sınıflandırıcısı, her bir sınıfın ait olma olasılığını Denklem 11'de belirtilen matematiksel ifadeye dayanarak hesaplar.

$$P(x \backslash C_k) = \prod_{i=1}^{n} P(x_i \backslash C_k) \tag{11}$$

Denklem 12'de $\boldsymbol{P(x)}$ tüm sınıflar arasında sabit olduğundan sınıf olasılıklarının karşılaştırılmasında genellikle hesaba katılmaz.

$$P(C_k \backslash x) = \frac{P(C_k) \prod_{i=1}^{n} P(x_i \backslash C_k)}{P(x)} \tag{12}$$

Denklem 13'de en yüksek olasılığa sahip sınıf, tahmin edilen sınıf olarak seçilmektedir.

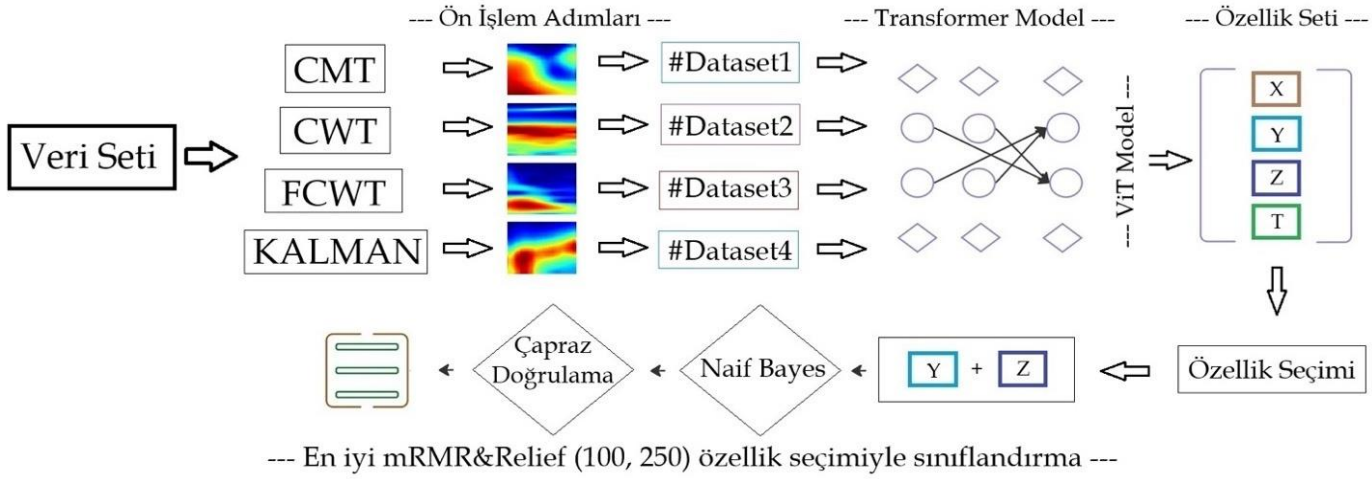
$$\hat{y} = \underset{C_k}{^{arg\,max P(C_k)}} \prod_{i=1}^{n} P(x_i \backslash C_k) \tag{13}$$

3.9. Önerilen Hibrit Yaklaşım

Bu çalışmada, fidye yazılımlarında görülen anomali ve sahte imzaların yüksek doğrulukla tespitini amaçlayan yapay zekâ temelli hibrit bir model önerilmiştir. Geliştirilen yaklaşım; ön işleme, model eğitimi, özellik çıkarımı, özellik seçimi ve sınıflandırma olmak üzere beş temel aşamadan oluşmaktadır. Ön işleme aşamasında, Kaggle platformunda sunulan ve gerçek fidye yazılımı etkinliklerini içeren açık erişimli bir veri seti kullanılmıştır. Veri setinde yer alan 1B sayısal verileri, zaman-frekans dönüşüm yöntemleri olan CMT, CWT, FCWT ve Kalman filtresi aracılığıyla 2B spektral görüntülere dönüştürülmüştür. Bu dönüşümler, fidye yazılımlarına özgü zaman-frekans desenlerinin daha görünür hale gelmesini sağlamıştır. Dönüştürülen her görüntü kümesi, bağımsız olarak ViT modeli ile eğitilmiştir. Görsel verilerdeki karmaşık örüntüleri yakalama kapasitesi nedeniyle tercih edilen ViT modeli ile her dönüşüm yöntemi için özgün ve derinlemesine özellik setleri üretilmiştir. Bu derin özellikler mRMR ve Relief algoritmaları kullanılarak işlenmiş böylece model başarısına en fazla katkıyı sağlayan öznitelikler belirlenmiştir. Özellik seçimi süreci ile yalnızca yüksek bilgi değeri taşıyan verilerin değerlendirilmesine olanak sağlayarak gereksiz veri yükü azaltmış böylece hem hesaplama maliyetinde düşüş hem de genel model performansında artış sağlanmıştır. En başarılı sonuçları sunan iki dönüşüme (CWT ve FCWT) ait özellik setleri birleştirilmiştir. Sınıflandırma aşamasında NB algoritması kullanılmış ve %99.3'lük yüksek bir başarı düzeyine ulaşılmıştır. Modelin doğruluk oranı, çapraz doğrulama yöntemiyle teyit edilmiştir. Önerilen ViT yaklaşımı, uçtan uca bir sınıflandırıcı olarak değil, yüksek düzeyli ve ayrıştırıcı temsiller

üreten bir özellik çıkarım modülü olarak kullanılmıştır. ViT'in kendi kendine dikkat mekanizması, zaman-frekans temsillerindeki doğrusal olmayan ve karmaşık örüntüleri öğrenerek bu örüntüleri sınıflar arası ayrımı güçlendiren yoğun bir özellik uzayına yansıtmaktadır [18,42].

Sonuç olarak, önerilen yaklaşım dalgacık dönüşüm tekniklerini, ViT tabanlı derin öğrenme modellerini, öznitelik seçimi algoritmalarını ve klasik makine öğrenmesi sınıflayıcılarını birlikte kullanarak fidye yazılımlarında anomali ve sahte imza tespitine yönelik güçlü, ölçeklenebilir ve güvenilir bir çözüm sunmaktadır. Önerilen modelin genel yapısı Şekil 3'te şematik olarak sunulmuştur. Şekil 3'te özellik seti bölümünde gösterilen X; CMT özellik setini, Y; CWT özellik setini, Z; FCWT özellik setini, T; Kalman filtresi özellik setini ifade etmektedir.



Şekil 3. Önerilen yaklaşım iş boru hattı.

4. Bulgular ve Tartışma

Deneysel çalışmalar kapsamında CMT, CWT, FCWT ve Kalman filtresi algoritmaları, Python programlama dili kullanılarak geliştirilmiş ve JupyterLab ortamında uygulanmıştır. Ön işleme adımları, Intel® Core™ i7 işlemci, Iris® Xe Graphics tümleşik grafik birimi ve 16 GB RAM kapasitesine sahip bir platformunda gerçekleştirilmiştir. Özellik birleştirme ve sınıflandırma süreçlerinde NB algoritması tercih edilmiştir. Elde edilen sonuçlar çapraz doğrulama yöntemi ile doğrulanmıştır. Model eğitimi aşamaları ise 3,40 GHz saat hızına sahip Intel® Core™ i7 işlemci, 32 GB RAM ve 10 GB grafik kartı kapasitesine sahip bir platformda yürütülmüştür. Deneysel performans değerlendirmeleri ise MATLAB 2024 yazılımı kullanılarak yapılmıştır. Çalışma bu yönleriyle sınırlıdır.

Analiz sonuçlarının yorumlanmasında karmaşıklık matrisi (confusion matrix) yöntemi kullanılmış; bu matrisin hesaplanmasında kullanılan metrikler ile ilgili formüller aşağıda detaylandırılmıştır. İlgili denklemler incelendiğinde, sınıflandırma sürecinin temel bileşenleri olan pozitif (P), negatif (N), doğru (T) ve yanlış (F) unsurlarının yer aldığı görülmektedir. Ölçme değerlendirme alanında yaygın biçimde kullanılan doğruluk metriği, özellikle dengeli veri kümeleriyle uygulandığında yüksek düzeyde başarı sağlamaktadır. Öte yandan, sınıf dağılımında dengesizlik bulunan veri kümelerinde F skoru metriği daha etkili ve anlamlı sonuçlar üretmektedir [43,44].

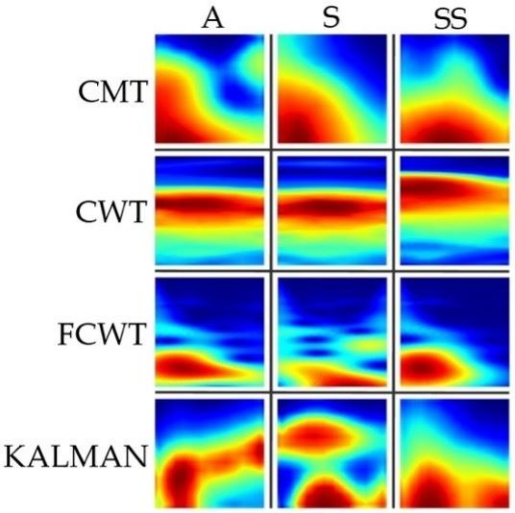
$$Doğruluk = \frac{TP + TN}{TP + TN + FN + FP} \tag{14}$$

$$F\ Skoru = \frac{2TP}{2TP + FN + FP} \tag{15}$$

$$Duyarlılık = \frac{TP}{FN + TP} \tag{16}$$

$$Kesinlik = \frac{TP}{TP + FP} \tag{17}$$

Bu çalışmada gerçekleştirilen deneysel analizler, üç aşamalı bir süreç çerçevesinde tasarlanmıştır. Birinci aşamada, veri setinde yer alan 1B sayısal veriler, ön işleme tabi tutularak 2B spektral görüntü formatında temsil edilmiştir. Bu işlem, transformer tabanlı modelin eğitim ve test süreçlerinde kullanılacak verinin hazırlanması amacıyla gerçekleştirilmiştir. Bu çalışmada bir sınırlılık olarak, veri setinin zaman-frekans bileşenleri yalnızca CMT, CWT, FCWT ve Kalman filtresi ile analiz edilmiş; diğer dalgacık dönüşüm teknikleri kapsam dışı bırakılmıştır. Elde edilen spektral görüntü kümelerinin örnekleri Şekil 4'te sunulmuştur.



Şekil 4. 1B sayısal verilerin CMT, CWT, FCWT ve Kalman filtresi yöntemleri kullanılarak 2B spektral görüntülere dönüştürülmesi ile elde edilen görüntü örnekleri.

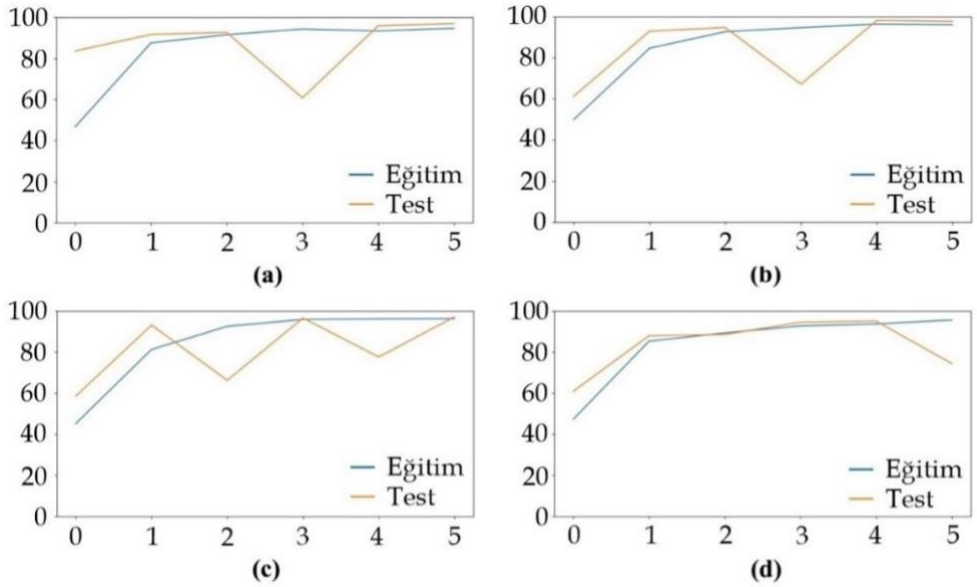
İkinci aşama, ön işlem süreci sonunda hazırlanmış olan dört farklı spektral görüntü kümesinin, önerilen model altında performansının değerlendirilmesini kapsamaktadır. Bu aşamada, literatürde son yıllarda tercih edilen ve diğer modellere kıyasla parametre sayısı bakımından daha verimli bir mimariye sahip olan ViT modeli kullanılmıştır. Model, her bir spektral görüntü kümesi için ayrı ayrı eğitilmiş, verilerin %70'i eğitim, %30'u ise test kümesi olmak üzere ayrılmıştır. Modelin eğitim süreci 6 devir (epoch) boyunca sürdürülmüştür. Çalışmada kullanılan ViT mimarisi sıfırdan eğitilmemiştir. Önceden eğitilmiş ağırlıklar kullanılarak transfer öğrenme yaklaşımı benimsenmiştir. Önceden eğitilmiş ViT modellerinde, düşük ve orta seviyeli görsel örüntülerin halihazırda öğrenilmiş olması nedeniyle, görece sınırlı sayıda epoch ile hızlı yakınsama elde edilmesi literatürde rapor edilen bir durumdur. Bu kapsamda uygulanan eğitim süreci, modelin tüm parametrelerini yeniden öğrenmekten ziyade, zaman-frekans temsillerinden elde edilen problem-özel örüntülere uyum sağlamayı amaçlayan bir ince ayar aşaması olarak tasarlanmıştır. Eğitim sırasında düşük öğrenme oranı kullanılmış ve erken yakınsama davranışı doğrulama eğrileri üzerinden izlenmiştir. Öğrenme eğrilerinin ilk birkaç epoch içerisinde doygunluğa ulaşması, veri setinin görece "aşırı kolay" olmasından ziyade, zaman-frekans tabanlı görselleştirmelerin sınıflar arası ayrımı belirginleştirmesi ve transfer öğrenmenin sağladığı temsil gücü ile açıklanmaktadır. Benzer biçimde, siber güvenlik ve sinyalden-görüntüye dönüşüm tabanlı çalışmalarda, önceden eğitilmiş transformer mimarilerinin 5–10 epoch aralığında kararlı performans sergilediği rapor edilmiştir [45]. Bu nedenle, çalışmada kullanılan epoch sayısı, literatürdeki çalışmalar incelendiğinde modelin eğitim stratejisi ve kullanılan öğrenme yaklaşımıyla tutarlı bir tercihtir.

ViT mimarisina ait parametreler Çizelge 4'te sunulmuştur. Modelin dört farklı spektral görüntü kümesi için elde ettiği eğitim ve test başarım grafikleri Şekil 5'te, oluşan karmaşıklık matrisleri ise Şekil 6'da sunulmuştur. Modelin performans metrikleri değerlendirilmiş ve Çizelge 5'te raporlanmıştır. Elde edilen sonuçlara göre, CMT tabanlı spektral görüntü kümesi %96.99 oranında, CWT tabanlı spektral görüntü

kümesi %97.78 oranında, FCWT tabanlı spektral görüntü kümesi %97.11 oranında, Kalman filtresi tabanlı spektral görüntü kümesi ise %74.33 oranında sınıflandırma başarısı sunmuştur. Bu bulgular, 2B spektral temsilinin ViT modeli tarafından etkili bir şekilde algılandığını ve analiz süreçlerinde kullanılabilir olduğunu göstermektedir.

Çizelge 4. Önerilen yaklaşımın parametre değerleri.

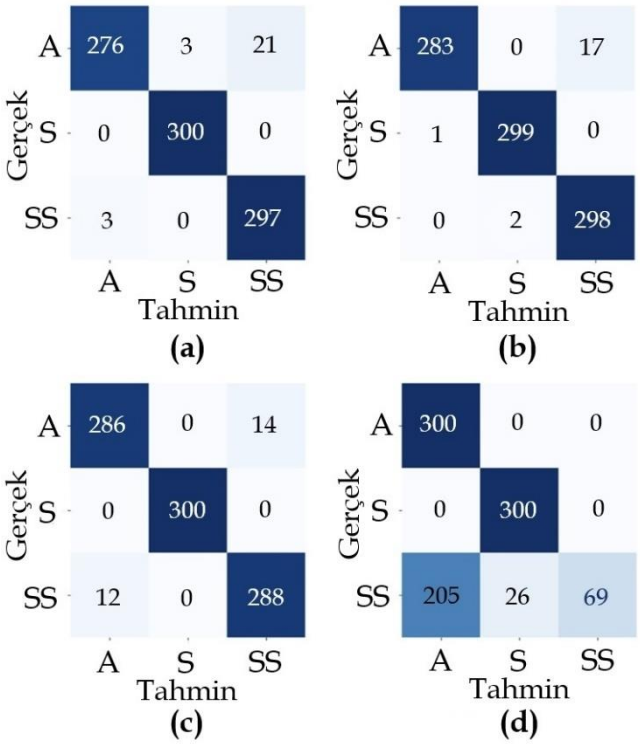
Model /Yöntem	Parametre	Tercih / Değer
ViT	Sınıflandırıcı	Linear
	Devir sayısı (epoch)	6
	Öğrenme oranı	1e-4
	Kayıp fonksiyonu	Cross Entropy
	Mini-toplu	16
	Optimizasyon	RMSprop
	Eğitim & Test oranı	%70 – %30
NB	On ayar	Gaussian Naive Bayes
	Dağıtım adı	Gaussian
	Tahmin hızı	-24000 obs/sec.
	Eğitim zamanı	0.98238 sec.
	Toplam maliyet	18



Şekil 5. ViT modelinin eğitim-test başarı grafikleri; a) CMT kümesi, b) CWT kümesi, c) FCWT kümesi, d) Kalman filtresi kümesi

Bu çalışmada ağ trafiğinden elde edilen öznitelikler, klasik anlamda zamansal sürekliliğe sahip fiziksel bir sinyal olarak değil, fidye yazılımı saldırılarının davranışsal dinamiklerini temsil eden çok boyutlu bir örüntü vektörü olarak modellenmiştir. Zaman-frekans dönüşümleri, bu tür davranışsal temsillerde ortaya çıkan ani ve lokal değişimleri ölçekler arası olarak görünür kılabilmektedir. Özellikle CWT dönüşümü, öznitelikler arasındaki mutlak sıralamadan ziyade, birlikte gerçekleşen göreli değişimleri frekans ve ölçek düzeyinde temsil ederek saldırı davranışlarının spektral imzalarını ortaya çıkarmayı amaçlamaktadır. Benzer şekilde, ağ trafiği analizi ve siber saldırı tespitinde zaman-frekans temsillerinin davranışsal anomalileri başarıyla ortaya koyduğu güncel çalışmalarda da raporlanmıştır. Fidye yazılımlarına ait sahte imzalar, gerçek saldırı imzalarından özellikle ağ trafiğinin zaman–frekans alanındaki davranışsal örüntüleri üzerinden ayrışabilmektedir. Gerçek fidye yazılımı saldırıları, ağ trafiğinde ani enerji yoğunlukları, düzensiz frekans dağılımları ve süreksiz spektral geçişler gibi belirgin dinamik özellikler üretir. Sahte imzalar ise bu örüntüleri çoğunlukla kısmi, zayıf veya yapay biçimde taklit etmektedir. Bu durum zaman-frekans temelli analizler ile öğrenme modelleri tarafından ayırt edilebilir davranışsal farklılıklar oluşturmaktadır. Zaman-frekans temsilleri, bu farkları zamansal veya istatistiksel yöntemlerin

yakalayamadığı ayrıntı düzeyinde görünür kılmaktadır. Özellikle CWT ve FCWT temsilleri, sahte imzalarda gözlenen spektral yoğunluk kopukluklarını ve tutarsız ölçek geçişlerini açık biçimde ortaya koymaktadır. CWT ve FCWT dönüşümleri, durağan olmayan sinyallerin zaman-frekans düzleminde ayrıntılı biçimde analiz edilmesini sağlar. Bu durum yalnızca sınıflandırma başarımını artıran özellikler sunmakla kalmaz, aynı zamanda sinyal davranışlarına ilişkin anlamlı spektral örüntülerin ortaya çıkarılmasına olanak tanır. CWT, farklı ölçeklerdeki geçici frekans bileşenlerini ve ani enerji yoğunluklarını yüksek çözünürlükle temsil ederken; FCWT, bu temsil gücünü koruyarak hesaplama verimliliğini ve gerçek zamanlı uygulanabilirliği artırmaktadır. Bu tür zaman-frekans temsillerinde, gerçek fidye yazılımı saldırılarına ait sinyaller belirli ölçeklerde yoğunlaşan enerji bantları ve süreksiz spektral geçişler sergilerken, normal veya sahte davranışların daha homojen ve düzenli spektral yapılar gösterdiği rapor edilmektedir [17,46]. Çalışmada, CWT temsillerinin FCWT'ye kıyasla daha kompakt ve gürültüye karşı görece daha dayanıklı spektral yapılar sunduğu görülmüştür. Buna karşılık FCWT, CWT'nin zaman-frekans çözünürlüğünü ve ayırt ediciliğini korurken hesaplama maliyetini düşüren ve ölçeklenebilirliği artıran optimize edilmiş bir dönüşüm sunmaktadır.



Şekil 6. ViT modelinin eğitimiyle elde edilen karmaşıklık matrisi; a) CMT kümesi, b) CWT kümesi, c) FCWT kümesi, d) Kalman filtresi kümesi.

Çizelge 5. Önerilen ViT modelinin analizlerinden elde edilen metrik sonuçlarının genel başarısı (%).

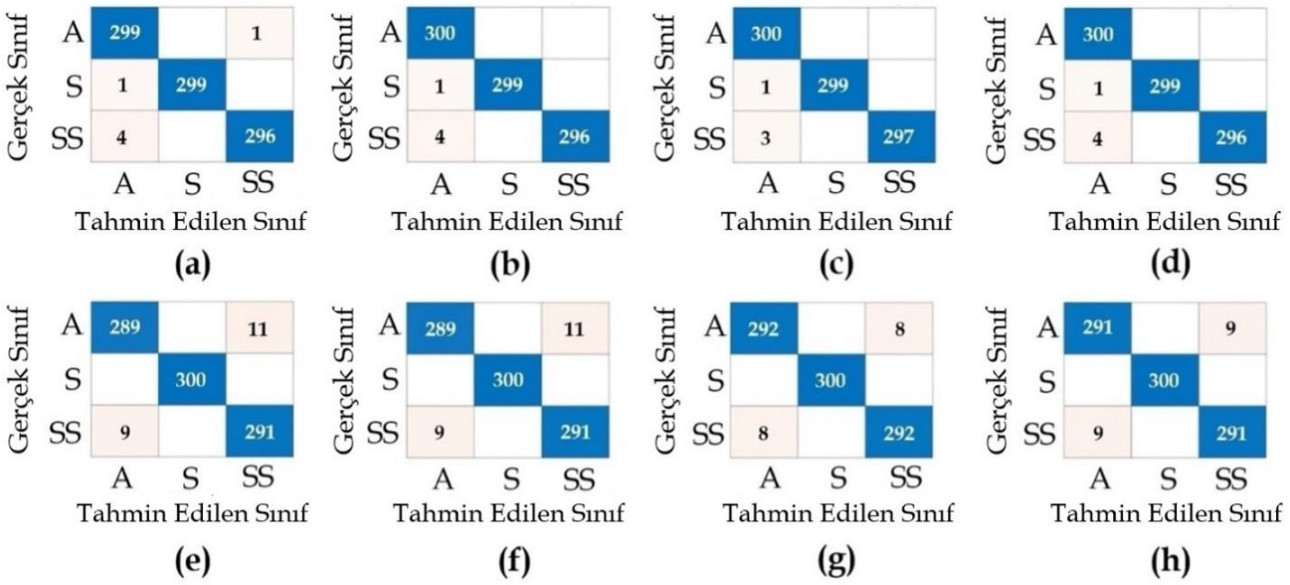
Veri kümesi	Duyarlılık	Kesinlik	F skoru	Doğruluk
CMT	97.0	97.1	97.0	97.0
CWT	97.8	97.8	97.8	97.8
FCWT	97.1	97.1	97.1	97.1
KALMAN	74.3	83.8	69.3	74.3

Deneysel sonuçlarda Kalman filtresi tabanlı dönüşümün, CWT ve FCWT'ye kıyasla daha düşük başarı göstermesi, yöntemin doğasıyla doğrudan ilişkili olabilir. Kalman filtresi, temel olarak doğrusal sistemlerde gürültü bastırma ve durum tahmini amacıyla tasarlanmış olup ani ve keskin değişimleri yumuşatma eğilimindedir [28]. Buna karşılık fidye yazılımı saldırıları, ağ trafiğinde ani ve süreksiz anomaliler oluşturmaktadır. Bu nedenle Kalman filtresi, saldırıya özgü bu ani sıçramaları gürültü olarak bastırarak ayırt edici imzaların silikleşmesine neden olabilir. CWT ve FCWT gibi zaman-frekans dönüşümleri ise lokal ve çok ölçekli değişimleri koruyarak saldırı örüntülerinin daha belirgin biçimde ortaya çıkmasını sağlamaktadır [46,47].

Üçüncü aşamada ViT modeli ile her bir görüntü kümesinden elde edilen özelliklerin, özellik seçimi yöntemiyle birleştirilmesi gerçekleştirilmiştir. Bu sürecin temel amacı modelin sınıflandırma performansını artırmak ve özellik seçiminin katkısını ortaya koymaktır. Bu doğrultuda ViT modelinin son katmanından, her bir görüntü için (görüntü sayısı x 768) boyutlarında özellik değerleri çıkarılmıştır. Söz konusu işlem dört farklı görüntü kümesi olan CMT, CWT, FCWT ve Kalman filtresi için ayrı ayrı uygulanmıştır. Yapılan değerlendirmeler sonucunda en yüksek başarıyı sağlayan iki görüntü kümesi (CWT ve FCWT) belirlenmiş ve yalnızca bu iki küme arasında özellik birleşimi gerçekleştirilmiştir. Her bir birleşim sonucunda; CWT için mRMR ve Relief sıralama algoritmalarıyla seçilen ilk 100 ve 250 özellikten oluşan setler, aynı şekilde FCWT için de elde edilmiştir. Modelin eğitimi sürecinde, veri seti %70 eğitim ve %30 test olacak şekilde ayrıştırılmıştır. Elde edilen bu özellik setlerinin sınıflandırma başarımını değerlendirmek amacıyla NB algoritması tercih edilmiştir. Çıkan sonuç çapraz doğrulama (k-cross validation) yöntemiyle ($k = 5$) teyit edilmiştir. Elde edilen sonuçların rastlantısal bir alt örneklemeye özgü olma riskini azaltmak amacıyla, deneylerde çapraz doğrulama uygulanmış ve farklı veri bölmeleri altında tutarlı performans elde edilmiştir. Bununla birlikte, modelin tüm veri seti üzerinde test edilmesi önemli bir hesaplama maliyeti gerektirdiğinden, bu durum çalışmanın temel sınırlılıklarından biri olarak değerlendirilmiş ve gelecekteki çalışmalar için açık bir araştırma yönü olarak ele alınmalıdır.

Elde edilen bulgular, çalışmanın odak noktasının fidye yazılımlarının ayırt edilmesinde zaman-frekans temsilleri ile transformer tabanlı öğrenme yaklaşımlarının sağladığı ayrıştırıcı gücün incelenmesi olduğunu ortaya koymaktadır. Literatürde, CWT gibi yöntemlerin sağladığı yüksek çözünürlüklü zaman-frekans temsillerin hesaplama açısından yoğun kaynak gerektirdiği bilinmektedir. Bu nedenle klasik CWT'nin çoğunlukla çevrimdışı analiz, yarı gerçek zamanlı izleme ve adli bilişim gibi statik veya işlem-yoğun senaryolarda etkin biçimde kullanıldığı rapor edilmiştir [25]. Bu çalışma kapsamında, CWT'ye kıyasla daha düşük hesaplama maliyeti sunan FCWT de değerlendirilmiştir. Deneysel sonuçlar, FCWT tabanlı zaman-frekans temsillerinin doğruluk açısından CWT ile karşılaştırılabilir performans sergilediğini ortaya koymuştur. Bu bulgu, yüksek doğruluk gereksinimi ile hesaplama verimliliği arasında denge kurulması gereken gerçek dünya senaryolarında FCWT'nin uygulanabilir bir alternatif olduğunu göstermektedir. Ayrıca, bu tür derin analiz yaklaşımlarının pratik sistemlerde genellikle hızlı imza tabanlı mekanizmalarla birlikte, çok katmanlı güvenlik mimarileri içerisinde ikincil bir analiz katmanı olarak konumlandırıldığı görülmektedir.

NB algoritmasının koşullu bağımsızlık varsayımının pratikte çoğu veri kümesinde tam olarak sağlanmadığı bilinmektedir. Literatürde bu varsayımın ihlal edildiği durumlarda dahi, öğrenilmiş veya derin temsillerle zenginleştirilmiş özellik uzaylarında NB'nin rekabetçi ve kararlı sınıflandırma performansı sergileyebildiği gösterilmiştir. Bu durum, klasik NB'nin görece basit yapısına rağmen, modern sınıflandırma problemlerinde etkili bir yöntem olarak kullanılabileceğini ortaya koymaktadır [48–50]. Bu çalışmada ViT çıktıları, mRMR ve Relief tabanlı özellik seçimi yöntemleriyle işlenerek korelasyonu azaltılmış ve sadeleştirilmiş bir özellik kümesi elde edilmiştir. Bu durum, NB'nin varsayımlarına pratikte daha uygun bir temsil uzayı oluşturmuştur. Ayrıca NB'nin düşük parametrik karmaşıklığı, sınırlı veri setlerinde aşırı öğrenme riskini azaltmakta ve olasılıksal yapısı sayesinde siber güvenlik uygulamalarında yorumlanabilir kararlar sunmaktadır. Yapılan karşılaştırmalı analizler, ViT+özellik seçimi+NB kombinasyonunun, ViT'in kendi sınıflandırma katmanına kıyasla daha kararlı sonuçlar sunduğunu göstermektedir. Sınıflandırma işlemi sonucunda oluşan karmaşıklık matrisleri Şekil 7'de, karmaşıklık matrisinin genel başarı yüzdesi ise Çizelge 6'da sunulmaktadır. NB algoritması ve çapraz doğrulama karmaşıklık matrisi metrikleri başarı yüzdeleri Çizelge 7'de sunulmuştur.



Şekil 7. Özellik setlerinin çıkarılmasıyla elde edilen karmaşıklık matrisleri; a) CWT; mRMR (100), b) CWT; mRMR (250) c) CWT; relief (100), d) CWT; relief (250), e) FCWT; mRMR (100), f) FCWT; mRMR(250), g) FCWT relief (100), h) FCWT relief (250).

Çizelge 6. Özellik seti birleşiminden elde edilmiş karmaşıklık matrisinin genel başarısı (%).

Görüntü Seti	Yöntem ve Özellik	Özellik Sayısı	Sınıf	Duyarlılık	Kesinlik	F skoru	Doğruluk
CWT	mRMR & Relief (100 & 250)	310	A	99.92	98.94	99.18	99.44
			S	99.67	99.92	99.79	
			SS	97.08	100.0	99.37	
FCWT	mRMR & Relief (100 & 250)	310	A	96.75	97.07	96.91	97.94
			S	100.0	100.0	100.0	
			SS	97.08	96.76	96.92	

Çizelge 7. Önerilen modelin NB ve Çapraz doğrulama metrikleri (%).

Sınıflandırıcı	Veri Tekniği	Sınıf	Duyarlılık	Kesinlik	F skoru	Doğruluk
NB	Eğitim-Test (0.7-0.3)	A	100.0	100.0	100.0	99.67
		S	99.67	100.0	99.84	
		SS	99.0	99.66	99.33	
	Çapraz doğrulama (k=5)	A	99.50	99.80	99.65	99.27
		S	99.70	99.60	99.65	
		SS	98.60	99.49	99.04	

5. Sonuç ve Öneriler

Bu çalışma, fidye yazılımlarında anomali ve sahte imza tespitine yönelik olarak zaman-frekans temelli dönüşüm teknikleri ile çoklu özellik seçimi yaklaşımının etkinliğini analiz etmeyi amaçlamaktadır. Araştırma sürecinde, 1B saldırı verileri sırasıyla CMT, CWT, FCWT ve Kalman filtreleme yöntemleri aracılığıyla 2B spektral görüntülere dönüştürülmüş ve bu görüntüler ViT mimarisiyle modellenmiştir. Elde edilen bulgular, söz konusu dönüşüm tekniklerinin spektral temsiller üzerinden elde edilen özellikleri zenginleştirdiğini ve bu durumun hem anomali hem de sahte imza tespitinde model başarımını belirgin şekilde artırdığını ortaya koymuştur. En yüksek başarı, CWT ve FCWT tabanlı özellik setlerinin

birleştirilmesi ve NB sınıflandırıcısı ile değerlendirilmesi sonucunda elde edilmiştir. Genel doğruluk oranı %99.3 olarak tespit edilmiştir. Bu sonuçlar çapraz doğrulama yöntemi ile teyit edilmiştir. Bulgular, çoklu özellik temsillerinin entegrasyonunun fidye yazılımlarının tespiti açısından önemli bir başarı unsuru olduğunu ortaya koymaktadır.

Bu çalışmada elde edilen sonuçlar, 1B verilerin zaman-frekans dönüşüm teknikleri aracılığıyla 2B spektral görüntülere dönüştürülmesinin ve farklı dönüşümlerden elde edilen görüntülerin bir araya getirilmesinin analiz doğruluğunu ve güvenilirliğini artırdığını göstermektedir. CMT, CWT, FCWT ve Kalman filtreleme yöntemleri tekil olarak yüksek doğruluk sağlasa da bu tekniklerin birlikte kullanıldığı özellik seçimi yaklaşımı sınıflandırma başarımını daha da iyileştirmiştir. Bu bulgu, anomali ve sahte imza tespiti gibi karmaşık siber güvenlik problemlerinde çoklu özellik entegrasyonunun etkili bir strateji olduğunu desteklemektedir. Ayrıca ViT mimarisinin parametrik verimliliği, sınırlı parametre sayısı ile yüksek doğruluk elde edilmesine katkı sağlamıştır. Bu durum, eğitim sürecinin optimize edildiğini ve hesaplama kaynaklarının etkin kullanıldığını göstermektedir.

Elde edilen bulgular, literatürde raporlanan başarı oranları ile genel olarak tutarlılık göstermektedir. Bununla birlikte, çalışmanın temel katkısı, 1B saldırı verilerinin 2B spektral görüntüler üzerinden işlenmesi ve bu temsillerin çoklu özellik seçimi ile desteklenmesiyle elde edilen yüksek sınıflandırma başarımıdır. Görüntü temelli yaklaşımların siber saldırı tespiti alanında sınırlı düzeyde ele alındığı dikkate alındığında, bu çalışma ilgili literatüre bütüncül bir bakış sunmaktadır. Bununla birlikte, kullanılan veri alt kümesinin boyutu, ViT tabanlı modellerin hesaplama gereksinimleri ve dönüşüm maliyetleri çalışmanın başlıca sınırlılıkları arasındadır. Bu nedenle önerilen yaklaşım, gerçek zamanlı ve mikrosaniye düzeyinde karar veren sistemlerden ziyade, çevrimdışı analizler, karar destek sistemleri veya canlı ortamlarda ikincil güvenlik katmanı olarak kullanıma daha uygundur. Gelecek çalışmalarda, daha büyük ve gerçek yaşamdan elde edilmiş veri setleri ile farklı transformer tabanlı mimarilerin ve özellik füzyon stratejilerinin değerlendirilmesi, modelin genellenebilirliğini ve uygulanabilirliğini artırabilir.

Teşekkür

Bu çalışma Fırat Üniversitesi Sosyal Bilimler Enstitüsü "Fidye Yazılımlarının Ağ Davranışlarında Anomali ve Sahte İmza Tespiti: Zaman-Frekans Temsilleri ve Transformer Tabanlı Bir Yaklaşım" başlıklı yüksek lisans tezinden türetilmiştir.

Katkı Beyanı

Burak Alperen BAHÇECİ: Literatür taraması ve değerlendirilmesi, veri analizi, verilerin ve analizlerin doğrulanması, model tasarımı, kodlama, bulguların yorumlanması, makalenin yazılması. Mesut TOĞAÇAR: Model tasarımı ve kodlama, bulguların yorumlanması, makale düzenleme.

Çıkar Çatışması Beyanı

Makalenin yazarları herhangi bir kurum, kuruluş, kişi ile kişisel ve finansal çıkar çatışması olmadığını beyan etmektedirler.

Kaynaklar

[1] Karaca MF, Erbey A, Parmaksız H, Fidan Ü. Yönetim bilişim sistemlerinde güncel konular. İstanbul: Özgür Yayınları; 2024. https://doi.org/10.58830/OZGUR.PUB498.

[2] Stallings W. Effective cybersecurity: understanding and using standards and best practices. Addison-Wesley; 2018. https://www.oreilly.com/library/view/effective-cybersecurity-a/9780134772929/ (Erişim tarihi: 08.05.2025)

[3] Çiçek AE. Türkiye'nin yapay zeka tabanlı siber güvenlik stratejisi: ulusal güvenliği güçlendirmek ve küresel siber yönetişime yön vermek. Yönetim Bilimleri Dergisi 2025; 23:993–1012. https://doi.org/10.35408/COMUYBD.1584175.
[4] Çelik S, Çeliktaş B. Güncel siber güvenlik tehditleri: fidye yazılımlar. Cyberpolitik Journal 2018; 3:105–132. https://dergipark.org.tr/tr/pub/cyberj/issue/39157/460303 (Erişim tarihi: 08.05.2025)
[5] Köksal M. Kamu güvenliği ve siber alan. Verimlilik Dergisi 2025; 27–29. https://edergi.sanayi.gov.tr/ (Erişim tarihi: 08.05.2025)
[6] AB Siber Güvenlik Ajansı (ENISA). Council, European Union - Consilium; 2024. https://www.consilium.europa.eu/en/ (Erişim tarihi: 08.05.2025)
[7] Zahra SR, Heeney S, Jakim B. UGRansome: optimal approach for anomaly intrusion detection and zero-day threats using cloud environment. [MSc thesis]. Dublin: National College of Ireland, School of Computing; 2022.
[8] Toğaçar M. Arşimet optimizasyon algoritması ile trafo tabanlı evrişimsel sinir ağı modelini kullanarak yazılım tanımlı ağ teknolojisi verilerinde saldırı tespiti. Fırat Üniversitesi Mühendislik Bilimleri Dergisi 2022; 34:341–349. https://doi.org/10.35234/FUMBD.1026610.
[9] Torky B. Ensemble methods for the anomaly detection in enterprise systems [MSc thesis]. Dubai: Rochester Institute of Technology; 2023.
[10] Igugu A. Evaluating the effectiveness of AI and machine learning techniques for zero-day attacks detection in cloud environments [MSc thesis]. Sweden: Luleå University of Technology; 2024.
[11] Yan P, Khoei TT, Hyder RS. A dual-stage ensemble approach to detect and classify ransomware attacks. In: 2024 IEEE 15th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON); 2024. p. 781–786. https://doi.org/10.1109/UEMCON62879.2024.10754695.
[12] Por LY, Dai Z, Leem SJ, Chen Y, Yang J, Binbeshr F, Phan KY, Ku CS. A systematic literature review on the methods and challenges in detecting zero-day attacks: insights from the recent CrowdStrike incident. IEEE Access 2024. https://doi.org/10.1109/ACCESS.2024.3455410.
[13] Kumar RVSA, Rayudu K, Kumar SR. Enhancing ransomware detection in cybersecurity: a comprehensive ensemble approach. Journal of Electrical Systems 2024; 20:5222–5232. https://doi.org/10.52783/JES.6235.
[14] Alzahrani S, Xiao Y, Asiri S, Alasmari N, Li T. RansomFormer: a cross-modal transformer architecture for ransomware detection via the fusion of byte and API features. Electronics 2025; 14:1245. https://doi.org/10.3390/electronics14071245.
[15] Mohamed AA, Al-Saleh A, Sharma SK, Tejani GG. Zero-day exploits detection with adaptive WavePCA-Autoencoder (AWPA) adaptive hybrid exploit detection network (AHEDNet). Sci Rep 2025; 15:4036. https://doi.org/10.1038/s41598-025-87615-2.
[16] Ghadami R. An intrusion detection system in the Internet of Things with deep learning and an improved arithmetic optimization algorithm (AOA) and sine cosine algorithm (SCA). Scientific Reports, 2025; 15. https://doi.org/10.1038/s41598-025-22074-3.
[17] Enisoglu R, Rakocevic V. A novel wavelet transform and deep learning-based algorithm for low-latency internet traffic classification. Algorithms, 2025; 18:457. https://doi.org/10.3390/A18080457.
[18] Takahashi S, Sakaguchi Y, Kouno N, Takasawa K, Ishizu K, Akagi Y, Aoyama R, Teraya N, Bolatkan A, Shinkai N, Machino H, Kobayashi K, Asada K, Komatsu M, Kaneko S, Sugiyama M, Hamamoto R. Comparison of vision transformers and convolutional neural networks in medical image analysis: a systematic review. Journal of Medical Systems, 2024; 48:84. https://doi.org/10.1007/s10916-024-02105-8.
[19] Nkongolo MW. UGRansome veri kümesi. Kaggle, n.d. https://www.kaggle.com/datasets/nkongolo/ugransome-dataset?resource=download (Erişim tarihi: 17.05.2025)
[20] Sonkar S. Transfer learning: leveraging pre-trained models for limited datasets through fine-tuning. International Journal of Information Technology and Management Information Systems, 2025; 16. https://doi.org/10.34218/IJITMIS_16_02_037.
[21] Jiang J, Zhang C, Ke L, Hayes N, Zhu Y, Qiu H, Zhang B, Zhou T, Wei GW. A review of machine learning methods for imbalanced data challenges in chemistry. Chemical Science, 2025; 16. https://doi.org/10.1039/D5SC00270B.
[22] Thölke P, Mantilla-Ramos YJ, Abdelhedi H, Maschke C, Dehgan A, Harel Y, Kemtur A, Mekki Berrada L, Sahraoui M, Young T, Bellemare Pépin A, El Khantour C, Landry M, Pascarella A, Hadid V, Combrisson E, O'Byrne J, Jerbi K. Class imbalance should not throw you off balance: choosing the right classifiers and performance metrics for brain decoding with imbalanced data. NeuroImage, 2023; 277:120253. https://doi.org/10.1016/j.neuroimage.2023.120253.

[23] Addison PS. The illustrated wavelet transform handbook: introductory theory and applications in science, engineering, medicine and finance. Boca Raton: CRC Press; 2017. https://doi.org/10.1201/9781315372556.
[24] Yan Y, Li QM. A general shock waveform and characterisation method. Mechanical Systems and Signal Processing, 2020; 136:106508. https://doi.org/10.1016/j.ymssp.2019.106508.
[25] Arts LPA, van den Broek EL. The fast continuous wavelet transformation (fCWT) for real-time, high-quality, noise-resistant time–frequency analysis. Nature Computational Science, 2022; 2:47–58. https://doi.org/10.1038/s43588-021-00183-z.
[26] Torrence C, Compo GP. A practical guide to wavelet analysis. Bulletin of the American Meteorological Society, 1998; 79:61–78. https://doi.org/10.1175/1520-0477(1998)079.
[27] Khairudin K, Hakim L, Nasution FH, Kurniawan R. The application of complex Morlet wavelet for estimating damping ratio and detecting inter-area oscillation mode on a real power system. In: Proceedings of the 2021 International Conference on Converging Technology in Electrical and Information Engineering; 2021. p. 1–4. https://doi.org/10.1109/ICCTEIE54047.2021.9650653.
[28] Welch G, Bishop G. An introduction to the Kalman filter. Chapel Hill: University of North Carolina; 2006. http://www.cs.unc.edu/~gb (Erişim tarihi: 12.05.2025)
[29] Soniya S, Sriharipriya KC. Integrating Kalman filter noise residue into U-Net for robust image denoising: the KU-Net model. Scientific Reports, 2024; 14:23641. https://doi.org/10.1038/s41598-024-74777-8.
[30] Çayıroğlu İ. Kalman filtresi ve programlama. 2012. http://www.ibrahimcayiroglu.com (Erişim tarihi: 01.06.2025)
[31] Dosovitskiy A, Beyer L, Kolesnikov A, Weissenborn D, Zhai X, Unterthiner T, Dehghani M, Minderer M, Heigold G, Gelly S, Uszkoreit J, Houlsby N. An image is worth 16x16 words: transformers for image recognition at scale. In: 9th International Conference on Learning Representations (ICLR 2021); 2020. https://arxiv.org/pdf/2010.11929 (Erişim tarihi: 24.01.2026)
[32] Devlin J, Chang MW, Lee K, Toutanova K. BERT: pre-training of deep bidirectional transformers for language understanding. In: Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics; 2019. p. 4171–4186. https://doi.org/10.18653/v1/N19-1423.
[33] Parvaiz A, Khalid MA, Zafar R, Ameer H, Ali M, Fraz MM. Vision transformers in medical computer vision—a contemplative retrospection. Engineering Applications of Artificial Intelligence, 2023; 122:106126. https://doi.org/10.1016/j.engappai.2023.106126.
[34] Tuncel İ, Albayrak A, Akın M. Öz dikkat mekanizması tabanlı görü dönüştürücü kullanılarak sıtma parazit tespiti. Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi, 2022; 13:271–277. https://doi.org/10.24012/DUMF.1120289.
[35] Khudhair Abbas Ali A, Aydın Y. Vision transformer-based approach: a novel method for object recognition. Karadeniz Fen Bilimleri Dergisi, 2025; 15:560–576. https://doi.org/10.31466/KFBD.1620640.
[36] Cıbuk M, Budak U, Guo Y, İnce MC, Şengür A. Efficient deep features selections and classification for flower species recognition. Measurement, 2019; 137:7–13. https://doi.org/10.1016/j.measurement.2019.01.041.
[37] Toğaçar M, Ergen B, Cömert Z. Detection of lung cancer on chest CT images using minimum redundancy maximum relevance feature selection method with convolutional neural networks. Biocybernetics and Biomedical Engineering, 2020; 40:23–39. https://doi.org/10.1016/j.bbe.2019.11.004.
[38] Aggarwal N, Shukla U, Saxena GJ, Rawat M, Bafila AS, Singh S, Pundir A. Mean-based relief: an improved feature selection method based on ReliefF. Applied Intelligence, 2023; 53:23004–23028. https://doi.org/10.1007/s10489-023-04662-w.
[39] Le TT, Urbanowicz RJ, Moore JH, McKinney BA. Statistical inference Relief (STIR) feature selection. Bioinformatics, 2019; 35:1358–1365. https://doi.org/10.1093/bioinformatics/bty788.
[40] Wang Q, Garrity GM, Tiedje JM, Cole JR. Naïve Bayesian classifier for rapid assignment of rRNA sequences into the new bacterial taxonomy. Applied and Environmental Microbiology, 2007; 73:5261–5267. https://doi.org/10.1128/AEM.00062-07.
[41] Rafdi A, Mawengkang H, Efendi S. Sentiment analysis using Naive Bayes algorithm with feature selection particle swarm optimization and genetic algorithm. International Journal of Advances in Data and Information Systems, 2021; 2. https://doi.org/10.25008/ijadis.v2i2.1224.
[42] Zhou H, Zou H, Li W, Li D, Kuang Y. HiViT-IDS: an efficient network intrusion detection method based on vision transformer. Sensors, 2025; 25:1752. https://doi.org/10.3390/S25061752.
[43] Karadeniz AT, Başaran E, Çelik Y. Classification of walnut dataset by selecting CNN features with whale optimization algorithm. Multimedia Tools and Applications, 2024; 83:77061–77076. https://doi.org/10.1007/s11042-024-18586-1.

[44] Hasnain M, Pasha MF, Ghani I, İmran M, Alzahrani MY, Budiarto R. Evaluating trust prediction and confusion matrix measures for web services ranking. IEEE Access, 2020; 8:90847–90861. https://doi.org/10.1109/ACCESS.2020.2994222.

[45] Kim HE, Maros ME, Miethke T, Kittel M, Siegel F, Ganslandt T. Lightweight visual transformers outperform convolutional neural networks for gram-stained image classification: an empirical study. Biomedicines, 2023; 11. https://doi.org/10.3390/biomedicines11051333.

[46] Purohit R, Kumar S, Sayyad S, Kotecha K. Time-frequency analysis and autoencoder approach for network traffic anomaly detection. MethodsX, 2025; 14:103228. https://doi.org/10.1016/j.mex.2025.103228.

[47] Huang H, Al-Azzawi H, Brani H. Network traffic anomaly detection. Cornell University, 2014. https://doi.org/10.48550/arXiv.1402.0856.

[48] Phatcharathada B, Srisuradetchai P. Randomized feature and bootstrapped Naive Bayes classification. Applied System Innovation, 2025; 8:94. https://doi.org/10.3390/ASI8040094.

[49] Peretz O, Koren M, Koren O. Naive Bayes classifier—an ensemble procedure for recall and precision enrichment. Engineering Applications of Artificial Intelligence, 2024; 136:108972. https://doi.org/10.1016/j.engappai.2024.108972.

[50] Zaidi NA, Jeś J, Cerquides J, Carman MJ, Webb GI. Alleviating Naive Bayes attribute independence assumption by attribute weighting. Journal of Machine Learning Research, 2013; 14:1947–1988. https://www.jmlr.org/papers/v14/zaidi13a.html.