2nd International Conference on Scientific and Academic Research
March 14-16, 2023 : Konya, Turkey
All Sciences Proceedings
http://as-proceeding.com/

E-postalarda Spam Kontrolü İçin QR Barkod Tekniğiyle işlenmiş Verilerin Artık Bloklu Derin Öğrenme Modelleriyle Analizi

Mesut Toğaçar[1*], Burhan Ergen[2]

[1]Yönetim Bilişim Sistemleri / İktisadi ve İdari Bilimler Fakültesi, Fırat Üniversitesi, Türkiye
[2]Bilgisayar Mühendisliği / Mühendislik Fakültesi, Fırat Üniversitesi, Türkiye

[*](mtogacar@firat.edu.tr) Başlıca yazarın mail adresi

Özet **–** Günümüzde e-posta hizmetleri şahsi, kurum ve kuruluşlar tarafından sıkça kullanılmaktadır. Kötü niyetli yazılımcılar kullanıcıların en çok tercih ettiği uygulamaları dikkate alarak yazılım geliştirirler. Bu tip yazılımcılar kullanıcılar üzerinden; hızlı para kazanma planlarını gerçekleştirmek, ürün / web sitesi reklamlarının tıklanmasını sağlamak, kişisel bilgilerin ele geçirilmesini sağlamak, bilgisayar sistemlerine zarar verme faaliyetlerinde bulunmak, vb. amaçları gerçekleştirebilmek için e-posta hizmetlerini de bu doğrultuda kullanabilmektedirler. E-posta hizmeti sunan sunucular veri güvenliğini ön planda tutmaktadır ve kullanıcılarına gelen e-postaları çeşitli yazılımlarla kontrol ederek filtreleyebilmektedir. Bazen bu tür yazılımlar dinamik alt yapıya sahip olmadıklarından dolayı istenmeyen e-postaları tespit edemeyebilir. Son zamanlarda e-postaların güvenliğini sağlayabilmek için yapay zekâ tabanlı yaklaşımlar kullanılmıştır. Bu çalışmada istenmeyen e-postaların (spam) denetimini gerçekleştiren hibrit bir yaklaşım sunulmuştur. Önerilen yaklaşımda kullanılan veri kümesi spam ve normal türündeki e-posta kayıtlarını içermektedir. Veri kümesindeki metin tabanlı kayıtlar QR barkod tekniği ile işlenerek iki boyutlu görüntü setleri oluşturulmuştur. Ardından, iki boyutlu QR görüntüler artık bloklu derin öğrenme modelleri (ResNet) ile eğitilmiştir. ResNet modellerin son katmanından elde edilen sınıf tabanlı özellik setleri birleştirilerek önerilen hibrit modelin başarı performansı artırılmıştır. Son adımda makine öğrenme yöntemi (en yakın komşu yöntemi) ile sınıflandırma işlemi gerçekleşmiştir. Çapraz doğrulama tekniği kullanılarak elde edilen sınıflandırma başarısı %99.91'di ve eğitim-test verisi oluşturularak gerçekleştirilen sınıflandırma başarısı %100'dü. Önerilen hibrit yaklaşımın istenmeyen e-postaların tespitinde başarılı sonuçlar verdiği yapılan bu çalışmada görülmüştür.

Anahtar Kelimeler – Spam, Derin Öğrenme, QR Kod, Özellik Birleştirme, Makine Öğrenme

I. GİRİŞ

Teknoloji çağında, bilgi paylaşımı ve kullanımı hızlı ve kolay bir şekilde gerçekleşmektedir. Kullanıcılar bu paylaşımı gerçekleştirirken çeşitli platformları (sosyal medya, e-posta, web siteleri, vs.) kullanabilmektedir. Bu platformların en eskileri arasında yer alan basit ve güvenli veri iletimi sağlayan elektronik posta (e-posta) hizmeti, günümüzde de kişisel ve/veya kurumsal işlemlerin gerçekleşmesinde sıkça tercih edilen bir dijital hizmet ürünüdür [1]. Spam, kötü amaçlı yazılımcılar tarafından tasarlanmış istenmeyen veya gereksiz e-postadır [2]. Spam olarak gönderilen e-postalar; bilgisayar korsanlığı, kimlik avı dolandırıcılığı, banka bilgilerine erişim, vb. amaçları gerçekleştirmek için tasarlanmıştır. Popüler olan e-mail sunucuları (Gmail, hotmail, yahoo, vb.) kullanıcılar tarafından daha çok tercih edilmektedir. Tercih edilmesinin en önemli nedenlerinden biri güvenli bilgi paylaşımı gelmektedir. Bazen spam kutularına düşmesi gereken e-postalar kullanıcılara doğrudan iletilebilmektedir [3]. Bütün bu gelişmeler gerçek zamanlı kontrolleri hızlı ve doğru bir şekilde gerçekleştirebilen sistemlere ihtiyaç duyduğunun göstergesidir.

Son zamanlarda yapay zekâ tabanlı yaklaşımlar kötü niyetli yazılımların tespitinde kullanılmış ve

gerçek zamanlı gerçekleştirilen bu analizlerde başarılı sonuçlar elde edilmiştir [4]. Spam ile ilgili gerçekleştirilen çalışmalar incelendiğinde; makine öğrenme yöntemlerini [1], [5]–[7], derin öğrenme modellerini [8]–[11] veri setlerine uygulayarak başarılı analizler gerçekleştirilmiştir. Bu bildiride sunulan yaklaşım ön işlem adımı, derin öğrenme ve makine öğrenme yöntemini birlikte işleyen hibrit bir model sunmuştur.

Bildirinin diğer bölümleri özetlenirse; veri kümesi hakkında bilgiler II. bölümde verilmiştir. Önerilen yaklaşımda kullanılan yöntem ve modellerin detaylı açıklaması III. bölümde yapılmıştır. Deneysel analizler ve sonuçları IV. bölümde yer almıştır. Tartışma ve Sonuç V. bölümde yer almıştır.

II. SPAM VERİ KÜMESİ

Veri kümesi, e-posta özelliklerini içeren sayısal verilerden oluşmuştur ve erişime açıktır. E-posta verileri iki sınıftan oluşmuştur. Bu sınıflar; spam ve normal. Veri kümesi 58 öznitelikten oluşmaktadır ve son öznitelik verinin etiketini belirler. Özniteliklerin bazıları kelime sayısı, harf sayısı, kesintisiz büyük harf sayısı gibi ölçümleri gerçekleştirir. Diğer özniteliklerde kelime frekansı, sayısal olmayan karakter sayısı, e-postadaki CHAR veri tipiyle eşleşen karakter sayısı, vb. bilgilerden oluşur. Veri kümesinde 1813 spam türü e-posta kaydı yer alırken, 2788 normal e-posta kaydı yer alır. Veri kümesi toplamda 4601 kayıttan oluşmaktadır [12].

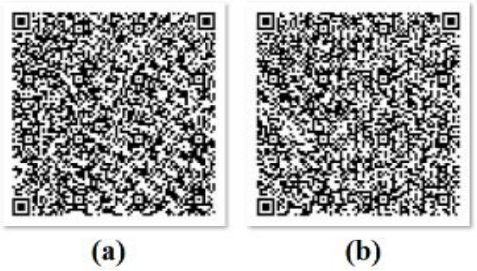
III. TEKNİK, YÖNTEM VE MODEL TASARIMI

Bu bölüm önerilen yaklaşımda kullanılan teknik, yöntem ve modeller hakkında bilgiler içermektedir.

A. *QR Barkod Tekniği*

QR kodu, 1B barkodların genişletilmesi sonucu oluşturulan 2B verileri saklayabilen bir barkod türüdür ve içerdiği bilgiler siyah beyaz dikdörtgen bir desen kullanılarak tarayıcı/okuyucu tarafından okunur. QR kodu, beyaz bir arka plan üzerinde matris biçiminde düzenlenmiş karelerden oluşur. Bu kodlar, geleneksel barkodlardan daha fazla veri içerebilir. Bunu yaparken dikey ve yatay kombinasyon düzenlemelerini kullanır. Bu sayede bilgi yoğunluğunu arttırır ve 1100-3800 bayt aralığında veri boyutunu destekler. Veri boyutu, çeşitli sıkıştırma algoritmaları kullanılarak artırılabilir. QR kodları ile 1B verilerin yanı sıra ses, grafik vb. içerikler de kodlanabilmektedir. Bu çalışmada orijinal veri kümesindeki 1B kayıtların her biri QR barkod tekniği kullanılarak 2B görüntülere dönüştürülmüştür [13].

Çalışmanın kod analizi Python dilinde gerçekleşmiştir [14]. 2B veri kümesine ait örnek görüntü kümesi Şekil 1'de gösterilmiştir.



Şekil 1. QR barkod tekniği ile oluşturulmuş örnek görüntüler; a) spam, b) normal.

B. *En Yakın Komşu Yöntemi*

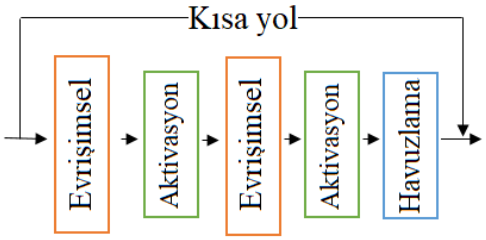
En yakın komşu (kNN) yöntemi, sınıflandırma işlemlerinde sıkça kullanılan denetimli bir makine öğrenme yöntemidir. Yöntemin algoritma yapısı, başlangıçta belirlenmiş veri noktasını dikkate alarak ilgili veri noktasının etrafındaki en yakın komşu verileri kullanarak işlem yapar. En yakın komşu verilerin sayısı k parametresi ile temsil edilir ve sorgulama da en yakın mesafelere göre bulunur. Bir sonraki adımda en yakın k veri noktası bulunur ve oylama gerçekleştirilir. Son durumda veri noktaları daha çok oy alan sınıfta gösterilir. Bu durum belirli bir iterasyon çerçevesinde tekrarlanır [15].

C. *Artık Bloklu Evrişimsel Model*

Evrişimsel sinir ağları (CNN) mimari yapısında evrişimsel, havuzlama ve tam bağlantılı katmanları bulundurur. Bu üç katman CNN modellerin ortak katmanı olarak bilinir. Evrişimsel katmanın görevi girdi görüntüsünü derinlemesine analiz ederek sayısal tabanlı özelliklerin çıkartılmasını sağlamak ve aktivasyon haritalarını oluşturmaktır[16]. Havuzlama katmanı ise esasen girdi boyutunu düşürterek CNN modelin eğitimini kolaylaştırmaktır. Tam bağlantılı katman CNN modelin son katmanlarını oluşturur ve sınıflandırma sürecine doğru giden özellikleri tek vektör formatında oluşmasını sağlar [17].

Artık bloklu evrişimsel model (ResNet), eğitim yakınsama hızını ve sınıflandırma doğruluğunu geliştirmek için tasarlanmış bir CNN modeldir. ResNet modellerin girdi boyutu 224×224 çözünürlüktedir. ResNet model; evrişimsel, havuzlama, artık bloklar ve softmax'tan oluşur. Artık blokların modele sunduğu katkı; girdi

verilerini kısa yol oluşturarak gereksiz olarak gördüğü bir ya da iki katmanı atlayıp ardından gelen katmana doğrudan aktarılmasını sağlamaktır. Bunun avantajı, modelin eğitim yakınsamasını hızlandırmak ve performans başarısını artırmaktır [18]. Artık blok tasarımı örneği Şekil 2'de gösterilmiştir.

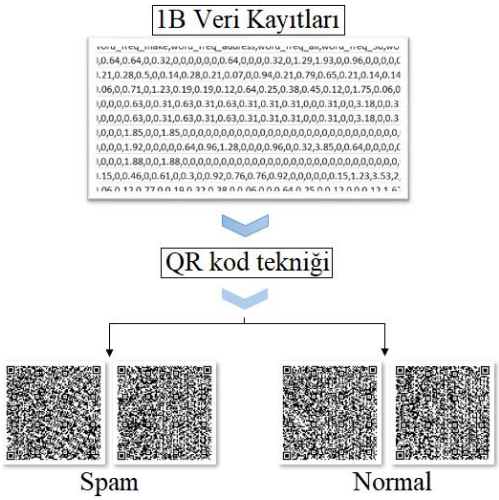


Şekil 2. Artık blok yapısının gösterimi.

Bu çalışmada ResNet model türlerinden ResNet-18 ve ResNet-50 modelleri kullanıldı.

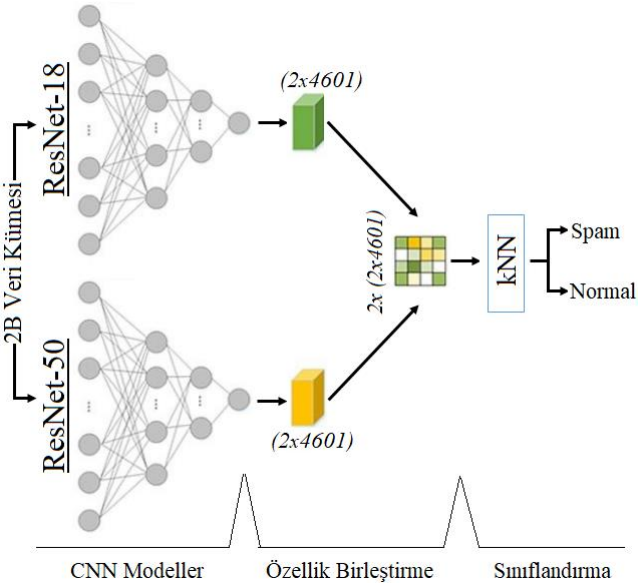
D. Tasarlanmış Hibrit Yaklaşım

Önerilen hibrit yaklaşım elektronik postalar üzerinden gönderilen spamların başarılı bir şekilde tespitini gerçekleştirmek için tasarlanmıştır. Önerilen yaklaşım önişlem adımı, model eğitimi ve özellik seti birleştirme adımlarından oluşmaktadır. Önişlem adımında 1B kayıtların QR barkod tekniği kullanılarak 2B görüntülere dönüştürülmesi sağlandı. Bu sayede 2B CNN modeller (ResNet-18, ResNet-50) tarafından eğitilmesi sağlandı. Bu dönüştürme işlemi Şekil 3'te gösterilmiştir.



Şekil 3. QR koda dönüştürme işlemi.

Model eğitiminde, 2B görüntü seti kullanılarak ResNet-18 ve ResNet-50 modelleriyle eğitimler gerçekleştirildi. Bu adımdaki amaç, modellerin son katmanında sınıf tabanlı özellik setlerini elde ederek bir sonraki adımda birleştirilmesini sağlamaktı. İki CNN modelden de iki adet sınıf tabanlı (sınıf sayısı × görüntü sayısı) özellik seti elde edildi. Son adımda iki özellik seti birleştirilerek (feature fusion), kNN yöntemi ile sınıflandırıldı. Özellik setlerinin birleştirilmesi işlemi genellikle önerilen modelin performans artışını sağlar. Bu çalışma için tasarlanmış hibrit yaklaşımın tasarımı Şekil 4'te gösterilmiştir.



Şekil 4. Tasarlanmış hibrit yaklaşım modeli.

IV. DENEYSEL ANALİZLER

Deneysel analizlerde CNN modellerin eğitimi, özellik birleştirme ve sınıflandırma işlemi Matlab2022 yazılımı kullanılarak gerçekleştirildi. Kullanılan donanım birimleri; Intel i5-3.10GHz işlemci, 16 GB geçici bellek ve 4 GB ekran kartıydı. Analizlerin nicel değerlendirilmesi için karmaşıklık matrisi kullanıldı. Karmaşıklık matrisinin doğruluk metriğinin hesaplanmasında Denklem 1 kullanıldı ve bu denklemde kullanılan; doğru (D), yanlış (Y), pozitif (P) ve negatif (N)'di [19]–[21]. Deneysel analizlerin gerçekleşmesinde kullanılan parametreler, Tablo 1'de verilmiştir.

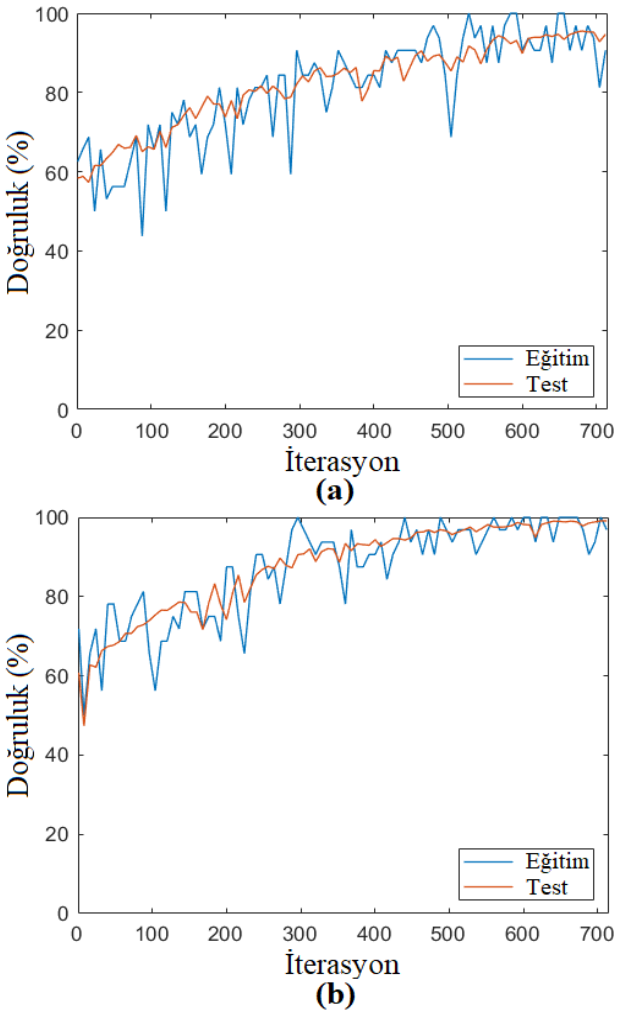
$$\text{Doğ.} = \frac{DP+DN}{DP+DN+YP+YN} \quad (1)$$

Deneysel analizlerin ilk adımında 1B veri kayıtları QR kod dönüştürme tekniği kullanılarak 2B barkod görüntüleri elde edildi. Ardından ResNet-18 ve ResNet-50 modelleri ile eğitildi. Eğitimin başarı grafikleri Şekil 5'te gösterilmiştir ve elde edilen karmaşıklık matrisleri Şekil 6'da gösterilmiştir. ResNet-18 modelin genel doğruluk

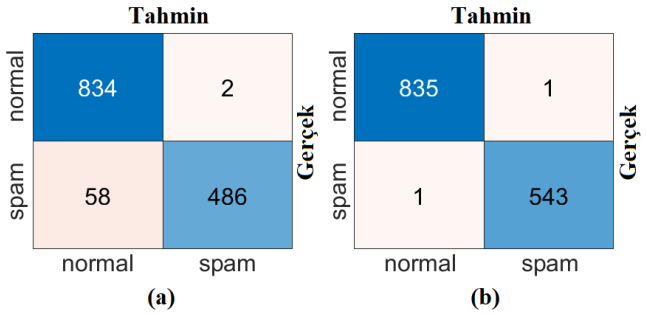
başarısı %95,65'ti ve ResNet-50 modelin genel doğruluk başarısı %99,86'ydı. ResNet-50 modeli ResNet-18 modele göre daha başarılı sonuç vermiştir. ResNet modelin derinliğinin artması başarı performansına da olumlu yansımıştır.

Tablo 1. Önerilen yaklaşımda tercih edilen parametre değerleri.

Model/ Yöntem	**Parametre**	**Değer/ Tercih**
ResNet-18 & ResNet-50	İterasyon sayısı	715
	Öğrenme oranı	1e-4
	Optimizasyon	SGD
	Sınıflandırıcı	Softmax
	Donanım kaynağı	Tekli GPU
	Mini – topluluk	32
	Eğitim/Test	0.7/0.3
kNN	Çapraz doğrulama (k)	10
	Eğitim/Test	0.7/0.3
	Mesafe metriği	Öklid
	Mesafe aralığı	Dengeli
	Komşu sayısı	100

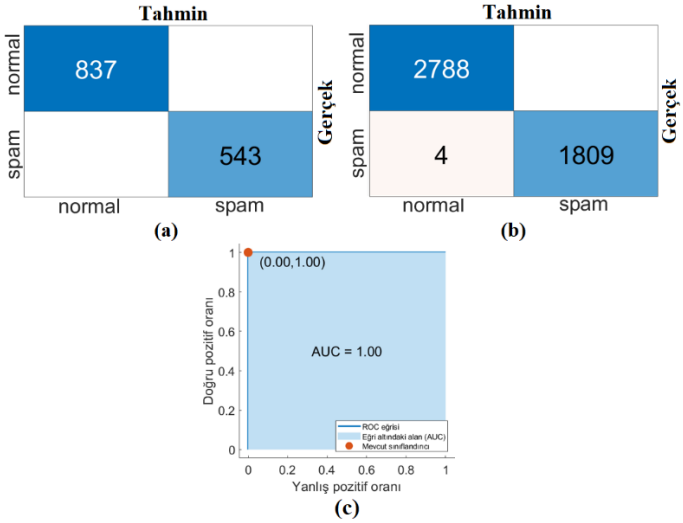


Şekil 5. CNN modellerin eğitimi;
a) ResNet-18, b) ResNet-50



Şekil 6. CNN modellerin karmaşıklık matrisleri;
a) ResNet-18, b) ResNet-50.

Deneysel analizlerin bir sonraki adımında ResNet-18 ve ResNet-50 modellerinden çıkartılan sınıf tabanlı özellik setleri (2×4601) birleştirilerek (4×4601) yeni bir özellik seti elde edildi. Birleştirilmiş özellik seti önce eğitim/test (0.7/0.3) şeklinde ayrılarak kNN yöntemi ile sınıflandırıldı. Sınıflandırma sonucunda %100 genel doğruluk performansı elde edildi. Ardından çapraz doğrulama tekniği kullanılarak (k=10), kNN yöntemi ile sınıflandırıldı. Bu işlem sonucunda elde edilen genel doğruluk başarısı %99.91 elde edildi. Bu analizlerin karmaşıklık matrisleri Şekil 7'de gösterilmiştir.



Şekil 7. Birleştirilmiş özellik setinin kNN yöntemi ile sınıflandırılmasından elde edilen karmaşıklık matrisleri;
a) test verisi (%30), b) çapraz doğrulama (k=10),
c) ROC eğrisi.

V. TARTIŞMA VE SONUÇ

Bulgular Bilgisayar kullanıcılarının çoğunun kişisel veya kurumsal e-postalarına gönderilen spamların tespitinde kullanılan filtre uygulamaları yetersiz kalabilmektedir. Gerçek zamanlı müdahalelerin yerinde ve zamanında olması

gerekir. Teknolojik gelişmeler, yapay zekâ tabanlı yaklaşımların bu tür eksikliklerin giderilmesi için alternatif olmuştur. Bu çalışmada spam verilerin tespitini başarılı şekilde gerçekleştirebilen ve çeşitli filtreleme yazılımlara uyum sağlayabilecek bir yaklaşım önerilmiştir. Önerilen yaklaşım, 2B-CNN modellerinin de metin tabanlı kayıtların analizinde başarılı olduğunu ispatlamıştır. 1B veri kayıtlarının QR barkod tekniği ile 2B görüntü verilerine dönüştürülmesi 2B-CNN modellerinin eğitiminin önünü açmıştır. Ayrıca bu çalışmada kullanılan ResNet modellerinin tercih edilmesinin sebebi, artık blok yapılarının evrişimsel katmanlar arasında sunmuş olduğu katkıdır. Özellik birleştirme tekniği birçok çalışmada performansı artırıcı bir yaklaşım içerdiği için bu çalışmanın son adımında özellik setlerine uygulandı. Sonuç olarak %100 genel doğruluk başarısı elde ettik ve önerilen yaklaşımımızın başarı performansını doğrulamak için çapraz doğrulama tekniğini de kullandık. Çapraz doğrulama tekniğiyle %99,91 genel doğruluk başarısı elde ettik. Bu sonuç, önerilen yaklaşımın analizlerini geçerli ve güvenilir kılmıştır. Sonuç olarak e-postalardan gelen spamların tespitinde önerilen yaklaşım, başarılı analizler gerçekleştirmiştir.

Gelecek çalışmada, diğer kötü amaçlı yazılım türlerinin yer aldığı veri kümeleri kullanılacaktır. Diğer barkod türlerine dönüştürülmesi gerçekleştirilecektir ve 2B-CNN modeller ile performansları karşılaştırılacaktır.

KAYNAKLAR

[1] N. Ahmed, R. Amin, H. Aldabbas, D. Koundal, B. Alouffi, and T. Shah, "Machine Learning Techniques for Spam Detection in Email and IoT Platforms: Analysis and Research Challenges," *Secur. Commun. Networks*, vol. 2022, pp. 1–19, Feb. 2022, doi: 10.1155/2022/1862888.

[2] F. Ahmad, S. Z. Yahya, Z. Saad, and A. R. Ahmad, "Tajweed Classification Using Artificial Neural Network," *2018 Int. Conf. Smart Appl. Commun. Networking, SmartNets 2018*, vol. 2, no. 11, pp. 8–14, 2018, doi: 10.1109/SMARTNETS.2018.8707394.

[3] K. Debnath and N. Kar, "Email Spam Detection using Deep Learning Approach," in *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON)*, May 2022, pp. 37–41. doi: 10.1109/COM-IT-CON54601.2022.9850588.

[4] M. S. Akhtar and T. Feng, "Malware Analysis and Detection Using Machine Learning Algorithms," *Symmetry (Basel).*, vol. 14, no. 11, p. 2304, Nov. 2022, doi: 10.3390/sym14112304.

[5] P. Malhotra and S. Malik, "Spam Email Detection Using Machine Learning and Deep Learning Techniques," *SSRN Electron. J.*, 2022, doi: 10.2139/ssrn.4145123.

[6] A. Rayan, "Analysis of e-Mail Spam Detection Using a Novel Machine Learning-Based Hybrid Bagging Technique," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–12, Aug. 2022, doi: 10.1155/2022/2500772.

[7] E. G. Dada, J. S. Bassi, H. Chiroma, S. M. Abdulhamid, A. O. Adetunmbi, and O. E. Ajibuwa, "Machine learning for email spam filtering: review, approaches and open research problems," *Heliyon*, vol. 5, no. 6, p. e01802, Jun. 2019, doi: 10.1016/j.heliyon.2019.e01802.

[8] G. M. Shahariar, S. Biswas, F. Omar, F. M. Shah, and S. Binte Hassan, "Spam Review Detection Using Deep Learning," in *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Oct. 2019, pp. 0027–0033. doi: 10.1109/IEMCON.2019.8936148.

[9] G. Chetty, H. Bui, and M. White, "Deep Learning Based Spam Detection System," in *2019 International Conference on Machine Learning and Data Engineering (iCMLDE)*, Dec. 2019, pp. 91–96. doi: 10.1109/iCMLDE49015.2019.00027.

[10] I. AbdulNabi and Q. Yaseen, "Spam Email Detection Using Deep Learning Techniques," *Procedia Comput. Sci.*, vol. 184, pp. 853–858, 2021, doi: 10.1016/j.procs.2021.03.107.

[11] A. S. Alhassun and M. A. Rassam, "A Combined Text-Based and Metadata-Based Deep-Learning Framework for the Detection of Spam Accounts on the Social Media Platform Twitter," *Processes*, vol. 10, no. 3, p. 439, Feb. 2022, doi: 10.3390/pr10030439.

[12] S. Sharma, "Spam Email Classification," *Kaggle Web*, 2020. https://www.kaggle.com/datasets/somesh24/spambase

[13] H. Wahsheh and F. Luccio, "Evaluating Security, Privacy and Usability Features of QR Code Readers," in *Proceedings of the 5th International Conference on Information Systems Security and Privacy*, 2019, pp. 266–273. doi: 10.5220/0007346202660273.

[14] P. Docourt, "django-qr-code 3.1.1," *PYPI*, 2022. https://pypi.org/project/django-qr-code/

[15] S. Uddin, I. Haque, H. Lu, M. A. Moni, and E. Gide, "Comparative performance analysis of K-nearest neighbour (KNN) algorithm and its different variants for disease prediction," *Sci. Rep.*, vol. 12, no. 1, p. 6256, Apr. 2022, doi: 10.1038/s41598-022-10358-x.

[16] M. Toğaçar, B. Ergen, and Z. Cömert, "Detection of weather images by using spiking neural networks of deep learning models," *Neural Comput. Appl.*, vol. 33, no. 11, pp. 6147–6159, Jun. 2021, doi: 10.1007/s00521-020-05388-3.

[17] A. Çalışkan, "Detecting human activity types from 3D posture data using deep learning models," *Biomed. Signal Process. Control*, vol. 81, p. 104479, Mar. 2023, doi: 10.1016/j.bspc.2022.104479.

[18] H. Wang, K. Li, and C. Xu, “A New Generation of ResNet Model Based on Artificial Intelligence and Few Data Driven and Its Construction in Image Recognition Model,” *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–10, Mar. 2022, doi: 10.1155/2022/5976155.

[19] E. Başaran, “A new brain tumor diagnostic model: Selection of textural feature extraction algorithms and convolution neural network features with optimization algorithms,” *Comput. Biol. Med.*, vol. 148, p. 105857, 2022, doi: https://doi.org/10.1016/j.compbiomed.2022.105857.

[20] A. Arı, “Brain MR Image Classification Based on Deep Features by Using Extreme Learning Machines,” *Biomed. J. Sci. Tech. Res.*, vol. 25, no. 3, Feb. 2020, doi: 10.26717/BJSTR.2020.25.004201.

[21] M. Toğaçar, Z. Cömert, and B. Ergen, “Enhancing of dataset using DeepDream, fuzzy color image enhancement and hypercolumn techniques to detection of the Alzheimer’s disease stages by deep learning model,” *Neural Comput. Appl.*, vol. 33, no. 16, pp. 9877–9889, Aug. 2021, doi: 10.1007/s00521-021-05758-5.