ADLİ TIP DERGİSİ
TURKISH JOURNAL OF FORENSIC MEDICINE

J For Med 2023;37(3):87–93
https://doi.org/10.61970/adlitip.2023.1208157
available online at: www.adlitipdergisi.com

DERLEME / REVIEW

COMPUTER FORENSICS

Dijital multimedya verilerinin güvenliği ve sahtecilik tespiti

Security of digital multimedia data and forgery detection

Fulya Akdeniz[1],
0000-0002-2303-5885

Yaşar Becerikli[2]
0000-0002-2951-7287

ÖZET

Dijital multimedya verilerinin bütünlüğünün doğrulanması konusundaki araştırmalar son yıllarda hız kazanmıştır. Buna bağlı olarak da dijital multimedya güvenliği üzerine yapılan çalışmaların sayısının gün geçtikçe arttığı gözlemlenmiştir. Bu da dijital multimedya güvenliği konusundaki çalışmaların hala güncel ve aktif bir araştırma alanı olduğunu göstermektedir. Ses, görüntü ve video alanlarında profesyonel bir eğitim almamış kişiler cep telefonları, akıllı cihazlar, çeşitli web uygulamaları vb. gibi araçlar üzerinden ses, görüntü ve video verileri üzerinde kolayca değişiklik yapabilmektedir. Yapılan bu değişiklikler ise verilerin doğruluğunu, bütünlüğünü ve gerçekliğini bozmaktadır. Bütünlüğü ve gerçekliği bozulmuş bu veriler adli makamları yanıltma, kamu düzenini bozma, mahkemede sahte delil olarak kullanma ve otomatik konuşmacı doğrulama sistemlerini yanıltma vb. gibi çeşitli amaçlar için kullanılabilmektedir. Bu sebepten günümüzde dijital multimedya verileri üzerinde yapılan sahteciliklerin tespit edilmesi oldukça önemli bir konudur. Yapılan çalışmalar, dijital multimedya verileri üzerindeki sahtecilik tespit yöntemlerini aktif ve pasif teknikler olmak üzere iki kategori altında toplamıştır. Literatürde özellikle ses sinyalleri başta olmak üzere dijital veriler üzerinde yapılan sahteciliklerin tespiti için aktif teknikler üzerine yoğunlaşıldığı pasif teknikler üzerine yapılan çalışmaların aktif tekniklere göre nispeten daha az olduğu tespit edilmiştir. Bu araştırma makalesinde pasif tekniklerden kopyala-yapıştır ve birleştirme sahtecilik tespitleri ile ilgili son yıllarda yapılmış olan çalışmaların kategorize edilmesi amaçlanmıştır. Bu çalışma dijital multimedya verilerinin güvenliği hakkında yapılan ilk Türkçe derleme çalışmadır.

Anahtar Kelimeler: *Dijital multimedya güvenliği, dijital multimedya adli bilişim, ses sahteciliği tespiti; görüntü sahteciliği tespiti, video sahteciliği tespiti*

ABSTRACT

Research on verifying the integrity of digital multimedia data has increasing in recent years. Therefore, it has been observed that the number of studies on digital multimedia security has increasing day by day. This shows studies on digital multimedia security are still an active research area. People who have not received professional training in the fields of audio, image and video can easily modify audio, image and video data through tools such as mobile phones, smart devices, various web applications, etc. These modifications disrupt the accuracy, integrity and authenticity of the data. These integrity and authenticity corrupted data can be used for various purposes such as misleading the judicial authorities, disrupting public order, using as fake evidence in court, and deceiving automatic speaker verification systems, etc. For this reason, it is very important forgeries detection systems on digital multimedia data today. Studies have gathered forgery detection methods on digital multimedia data under two categories as active and passive techniques. In the literature, studies on passive techniques, which focus on active techniques for forgery detection on digital data, especially on audio signals, are relatively less than active techniques. In this research article, it is aimed to categorize the recent studies on copy-move and splicing forgery detection from passive techniques. This study is the first Turkish review on the digital multimedia data security.

Keywords: *Digital multimedia security, digital multimedia forensic, audio forgery detection, image forgery detection, video forgery detection*

Cite as: Akdeniz F, Becerikli Y. Dijital multimedya verilerinin güvenliği ve sahtecilik tespiti. J For Med 2023;37(3):87–93

Received: 03.02.2023 • **Accepted:** 17.09.2023

Corresponding Author: Fulya Akdeniz, Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü,Kocaeli, Türkiye
E-mail: fulya.akdeniz@kocaeli.edu.tr

[1]Arş. Gör., Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü, Kocaeli, Türkiye
[2]Prof. Dr., Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü, Kocaeli, Türkiye

GİRİŞ

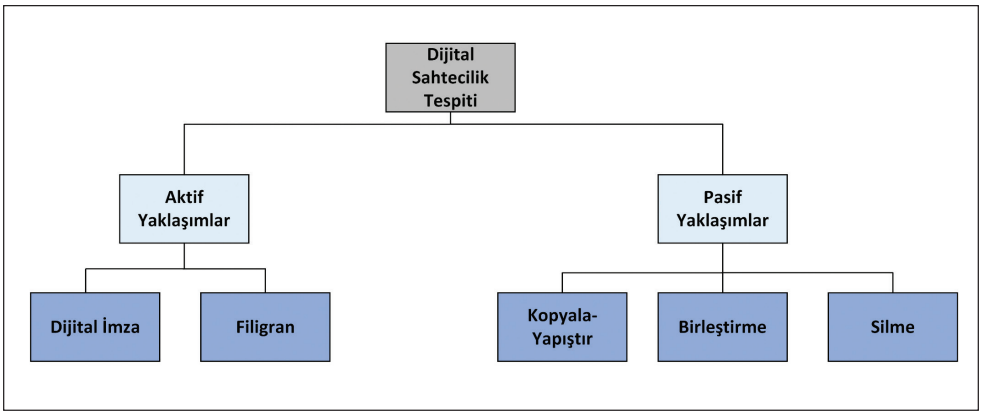
Dijitalleşme; analog bilgilerin alınarak bilgisayarların bu bilgileri depolayabilmesi, işleyebilmesi ve iletebilmesi için bu bilgilerin sıfır ve bir olarak ifade edilip kodlanmasıdır. Dijitalleştirme ise bilgilerin ve verilerin dijital bir ortama aktarılarak analog formdan dijital forma geçişini ifade eder (1). Teknolojinin ve internetin yaygınlaşması ile web ortamları, sanal ortamlar ve sosyal ağlarda üretilen veri miktarları her geçen gün artmaktadır. Bu durum ortaya milyonlarca ses, görüntü, video ve metin gibi multimedya verilerinin oluşmasına olanak tanımıştır. Dijital multimedya verilerine çeşitli platformlar üzerinden kolayca ulaşılabilmesi dijital multimedya güvenliğine duyulan ihtiyacı da artırmıştır. Dijital multimedya güvenliği (Digital Multimedia Security), dijital multimedya verileri/kaynakları üzerinde yapılan herhangi bir manipülasyon/sahtecilik işlemini konu alan bir bilim dalıdır. Dijital multimedya güvenliği konusu veri çeşitliliğinin ve veri boyutunun sürekli olarak artmasından dolayı sürekli geliştirilmesine ihtiyaç duyulan bir çalışma alanı olmuş ve olmaya devam etmektedir. Dijital multimedya verileri, biyometrik kimlik doğrulama, askeri, savunma, adli makamlar gibi stratejik birçok alanda kullanıldığı için bu verilerin bütünlüğünün ve güvenilirliğinin doğrulanması çok kritik bir konudur (2).

Son yıllarda görüntü, video ve ses düzenleme araçlarının sayısı artmıştır. Bu artış sahte dijital multimedya verilerinin üretilmesini de arttırmıştır. Mobil telefonlar ve uygulamalar dahil birçok dijital multimedya araçları aracılığıyla bu veriler üzerinde çeşitli düzenleme, değişikliklerin yapılması ve bu tür düzenleme araçlarının kullanımlarının kolaylaşması sayesinde medya, web ve sosyal platformlar üzerinde büyük miktarda sahte/değiştirilmiş/kurcalanmış/manipülasyon işlemlerine uğramış dijital multimedya verisi ortaya çıkmıştır. Bu işlemler verilerin anlamsal içeriklerini değiştirmektedir. Bu içerik değişimi iyi niyetli yapılabildiği gibi kötü niyetli olarakta yapılabilmektedir. Büyük sosyal ağ platformları 2022 yılından itibaren manipülasyona uğramış verileri tespit edip bunları filtrelemek için çok daha fazla çaba sarf etmektedir. Çünkü yapılan bu manipülasyon işlemleri ile insanlar kolayca kandırılıp tehdit edilebilmektedir (3).

Dijital multimedya verileri üzerinde yapılan sahtecilik tespiti temel olarak aktif ve pasif olmak üzere ikiye ayrılır. Aktif teknikler, orjinal veriden dijital filigran (watermark), dijital imza (signature), hash gibi özel bilgileri analiz ederek sahtecilikleri tespit etmektedir. Pasif teknikler ise veri ve verinin özelliklerini kullanarak sahtecilik tespitine odaklanan tekniklerdir. Aktif teknikler, dijital filigran ve dijital imza gibi ek bilgilere ihtiyaç duymaktadır. Fakat kullanılan her dijital multimedya verisinde bu bilgilerin bulunması beklenemez, bu problem aktif tekniklerin en büyük dezavantajı ve güçsüz yönüdür. Pasif tekniklerde ise sahteciliğin tespit edilmesi aktif tekniklere kıyasla daha zordur (1,4,5).

Kullanılan dijital multimedya verisi hakkında daha önceden bilginin olup olmaması durumuna göre sahteciliği tespit etmede kullanılan teknikler değişmektedir. Veri, dijital imza ve dijital filigranı içeriyorsa aktif teknikler kullanılabilir. Veri hakkında herhangi bir bilgi bulunmadığı durumlarda ise aktif teknikler güçsüz hale gelip pasif tekniklere odaklanılması gerekir. Bu sebepten aktif ve pasif teknikler kullanılarak sahteciliğin tespit edilmesi oldukça önemli bir durumdur (6). Dijital sahtecilik tespitine yönelik kullanılan yöntemlerin kategorize edilmiş haline Şekil 1'de verilmiştir.

Dijital adli bilişim ses, görüntü ve video gibi dijital verilerin içeriklerinin korunması, verilerin bütünlüğü ve doğrulanması için çeşitli çalışmalar yaparak dijital multimedya verileri üzerindeki sahtecilikleri tespit eden günümüzde aktif ve hala gelişmekte olan bir çalışma alanıdır (7,8,9). Dijital adli bilişim günümüzde mahkemelerdeki çeşitli davalarda kullanılmaktadır. Dijital adli bilişim alanında yapılan çalışmalar incelendiğinde görüntü ve video alanında yapılan çalışmaların ses alanında yapılan çalışmalara kıyasla daha önce başladığı görülmüştür. Ses sahteciliklerini tespit eden çalışmaların ise yeni gelişmekte olup hala başlangıç aşamasında olduğu tespit edilmiştir. Dijital adli bilişim, bilgisayarların ve internetin yaygınlaşması ile 2000'li yılların başında gelişmeye başlamıştır. İlk yıllarda toplanan kanıtlar bilgisayar tabanlı olduğu için ilk önce bilgisayar adli bilişim (computer forensic) olarak adlandırılmıştır. Ancak son yıllarda teknolojinin ilerlemesi ile birlikte çeşitli teknolojik ürünler ortaya çıkmıştır. Bu teknolojik ürünler ile hem dijital kanıt



Şekil 1. Dijital sahtecilik tespiti yaklaşımları

üretilmekte hem de cihazın kendisi kanıt niteliği taşımaktadır. Son yıllarda dijitalleşmenin her alana girmesiyle bilgisayar adli bilişim kavramı dijital adli bilişim olarak adlandırılmış ve literatürde bu isimle yer almaya başlamıştır. Dijital adli bilişim, bir dijital multimedya verisinin olay yerinde delil olarak tanımlanması ile başlayıp mahkemelerde delil olarak ortaya sunulmasına kadar olan bir çok farklı aşamaya sahip olan bir süreçtir (10).

Literatürde dijital multimedya verileri üzerinde yapılan değişiklikler sahtekarlık (forgery), kurcalama (tampering) ve manipülasyon (manipulation) gibi çeşitli isimlerle adlandırılmışlardır. Bu tanımlamaların her biri ile kast edilen veri üzerinde yapılmış olan değişikliklerdir.

Literatürde dijital multimedya verileri üzerinde yapılan sahtecilik tespitlerinin en çok görüntü, video ve ses verileri üzerine odaklandığı görülmüştür. Bu durumdan görüntü, video ve ses verileri üzerinde yapılan sahtecilik tespitinin önemi görülmektedir. Görüntü, video ve ses üzerinde yapılan kopyala-yapıştır ve birleştirme sahtecilik tespitleri ise diğer sahtecilik tespitlerine göre nispeten daha zordur. Bu sahtecilikler verideki anlam bütünlüğünü değiştirebildiği için tespiti diğer sahtecilik türlerine göre daha kritik bir noktadadır. Bu çalışma ses, görüntü ve video üzerinde yapılan kopyala-yapıştır ve birleştirme sahtecilik tespitleri ve bu sahtecilik tespit yöntemleri hakkında bir çalışma sunmaktadır. Bu amaçla çalışmanın ilk aşamasında temel dijital multimedya kavramlarının tanımları ve yapılan uygulamalar hakkında genel bir bakış sunulmuştur. İkinci aşamada literatürdeki güncel sahtecilik tespiti çalışmalarına yer verilmiştir. Son aşamada ise sonuç kısmı anlatılmıştır.

İLGİLİ ÇALIŞMALAR

Görüntü Tabanlı Sahtecilik

Kopyala-yapıştır sahteciliği işleminde, herhangi bir görüntünün belirli bir bölümü seçilerek bu bölümün aynı görüntü üzerinde başka bir bölüme kopyalanıp yapıştırma işlemi gerçekleştirilir. Böylece, görüntünün bu iki bölümünün korelasyon değeri görüntünün diğer bölümlerine göre nispeten daha yüksek olacaktır. Bir nesnenin benzer piksel bölümleri aynı görüntüde aynı boyutlara, benzer geçişlere ve benzer dokulara sahip olduğundan daha kolay algılanabilir. Bu sebeple kopyala-yapıştır görüntü sahteciliği yapılmış görüntülerdeki sahtecilikleri algılamak görüntü birleştirme sahteciliğini algılamaktan daha kolaydır. Görüntü birleştirme sahteciliğinde ise görüntüdeki farklı dokular, farklı boyutlar ve piksellerin geçişlerinin niteliklerinin farklı olması ile nesneler tanıtılır. Bu sebeple görüntü birleştirme sahteciliğinde sahteciliği tanımlamak zorlaşır (11).

Qazi vd., 2022 çalışmalarında ResNet50v2 mimarisini kullanarak görüntü birleştirme sahteciliğini tespit çalışması yapmışlardır. Çalışmalarında önerilen model, girdi olarak görüntü yığınlarını almakta ve başlangıç olarak YOLO ağırlıklarını ResNet50v2 mimarisine vererek görüntü birleştirmeyi tespit etmektedir. Bunun için orijinal ve sahte olmak üzere

iki farklı kategori içeren CASIA_v1 ve CASIA_v2 veri kümeleri kullanılmıştır. Sonuçta CASIA_v2 veri kümesi, CASIA_v1 veri kümesine kıyasla daha kapsamlı olduğu için transfer öğrenme kullanılarak ince ayarlı model için %99,3 ve CASIA_v2 veri kümesi ile transfer öğrenme olmadan %81 doğruluk elde etmişlerdir (12).

Ali vd., 2022 çalışmalarında hem görüntü birleştirme sahteciliği tespiti için hem de kopyala yapıştır sahteciliği tespiti için bir sistem geliştirdiler. Bu sistem minimum parametrelerle tam bağlantılı bir katmanın olduğu 3 evrişim katmanından oluşan çok hafif bir CNN modelidir. Yazarlar önerilen model performansının son teknoloji yaklaşımlardan daha hızlı ve hafif olduğu vurgulamışlardır. Deneysel çalışmada, %92,23 doğruluk oranı elde edilmiştir (13).

Fatima vd., 2022 çalışmalarında kopyala-yapıştır sahtecilik teknikleri kullanarak iki adımlı bir kilit nokta tabanlı sahtecilik tespit tekniği sunmaktadır. Yazarlar çalışmalarında düzgün bölgelerdeki anahtar noktaları algılamak için SIFT algoritmasını, eksik bölgelerden anahtar noktaları tespit etmek için FAST tanımlayıcılara sahip BRIEF özelliklerini kullanmışlardır. Simülasyon sonuçlarına göre önerilen tekniğin iyi görsel sonuçlar verdiği ve hesaplama karmaşıklığını azalttığı tespit edilmiştir (14).

Rodriguez-Ortega vd., 2021 çalışmalarında kopyala-yapıştır sahteciliği tespiti için derin öğrenmeyi kullanan özel bir mimariye sahip bir model (copy-move forgery detection-CMFD) ve bir transfer öğrenme modeli (VGG-16) geliştirmişlerdir. Her durum için ağın derinliğinin etkisini kesinlik (P), hatırlama (R) ve F1 puanı açısından analiz etmişler ve genelleme sorununu sekiz farklı açık erişim veri kümesinden alınan görüntülerle ele almışlardır. Modeller, değerlendirme ölçütleri, eğitim ve çıkarım süreleri açısından karşılaştırılmış ve VGG-16 transfer öğrenme modelinin, özel bir mimari ile modelden yaklaşık %10 daha yüksek metrikler elde ettiğini ortaya koymuşlardır ve ikincisinden yaklaşık iki kat daha fazla çıkarım süresi gerektiğini söylemişlerdir (15).

Manjunatha vd., 2021 çalışmalarında derin öğrenme tekniklerini kullanarak pasif görüntü sahteciliği (kopyala yapıştır ve görüntü birleştirme sahtekarlıkları) tespit etmişlerdir. MICC, CASIA ve UCID vb. gibi farklı görüntü sahtekarlığı veri kümeleri kullanılmıştır. Önerilen CNN tabanlı sahtecilik algılama yönteminin, mevcut sahtekarlık algılama yöntemleri ile performansı değerlendirilmiştir (16).

Barad vd., 2020 çalışmalarında kopyala yapıştır ve görüntü birleştirme sahtecilikleri tespiti için geleneksel yöntemlerdeki problemleri vurgulamışlardır. Geleneksel görüntü sahteciliği tespiti yaklaşımlarındaki sorunun, görüntüdeki sadece belirli özelliklerin tanımlanması olduğunu vurgulamışlardır. Bu sebeple çalışmalarında derin öğrenme yöntemleri kullanılarak görüntüden karmaşık öznitelikleri çıkarmışlar ve geleneksel yöntemlerden daha iyi bir doğruluk oranı elde etmişlerdir. Çalışmalarında sahte görüntü tespiti için derin öğrenme tabanlı tekniklerin ayrıntılı bir araştırmasını, analizini, bulgularını ve halka açık görüntü sahteciliği veri kümelerini ayrıntılarıyla anlatmışlardır (17).

Video Tabanlı Sahtecilik

Videolarda kopyala-yapıştır sahteciliği video içerisinde bulunan nesnelerle ilgilidir. Bu tür sahteciliklerde, videodaki nesneler aynı videodaki diğer karelere kopyalanır ve yapıştırılır. Video ekleme sahteciliği, bir videonun bazı bölgelerine başka bir videodan bölgelerin kopyalanması anlamına gelir. Çalışmaların birçoğu görüntü ekleme üzerine yoğunlaştığı için bu alanda da sınırlı sayıda çalışma bulunmaktadır (18,19).

Patel vd., 2022 çalışmalarında görüntü ve video sahtecilik teknik ve tespitlerini incelemişlerdir. Özellik karşılaştırma ve RANSAC kullanarak kopyala-yapıştır sahtecilik tespiti için pasif video sahteciliği algılama tekniklerini geliştirmişlerdir. Yazarlar çalışmalarında çerçeveler üzerinde değişiklik yapılmış çerçeveleri ayırt etmek için iki hesaplama aşaması tanımlamışlar ve özellik çıkarma aşamasında korelasyon yöntemini kullanarak, değiştirilen çerçeveleri ayırt etmişlerdir. Tüm video akışı boyunca sahtecilik olan karelerdeki değişikliklerin ölçüsünü kontrol etmek için her kare, hesaplanan özelliklere göre bir önceki ve sonraki karelerle karşılaştırılmıştır (19).

Raskar vd., 2022 çalışmalarında videolar üzerinde yapılan kopyala-yapıştır sahteciliğini tespit etmişlerdir. Bu çalışmada, kopyala-yapıştır sahteciliği tespiti için YOLOv2 yöntemini kullanmışlardır.. Deneysel analiz sonucunda, önerilen YOLOv2 modelinin ölçekleme, döndürme, çevirme gibi kopyala-yapıştır saldırılarını tespit etmek için iyi sonuçlar elde etttiği tespit edilmiştir (20).

Shelke vd., 2021 çalışmalarında pasif teknikler kullanılarak video sahteciliği tespiti üzerine kapsamlı bir araştırma sunmuştur. Bu çalışmanın birinci amacı, mevcut pasif video sahteciliği tespit tekniklerini incelemek ve analiz etmektir. İkinci amacı standart kıyaslama video sahteciliği ve pasif video sahteciliği tespit teknikleri için genelleştirilmiş mimarileri tartışmaktır (21).

Fadl vd., 2021 çalışmalarında derin otomatik özellik çıkarımı için uzamsal-zamansal bilgi ve füzyonun 2B evrişim sinir ağı (2B-CNN) kullanan çerçeveler arası sahtecilik (çerçeve silme, çerçeve ekleme ve çerçeve çoğaltma) tespit sistemi önermişlerdir. Sınıflandırma işlemi için Gaussian RBF çok sınıflı destek vektör makinesi (RBF-MSVM) kullanılmıştır. Deneysel sonuçlar, sahte videolar Gauss gürültüsü, Gauss bulanıklaştırma, parlaklık modifikasyonları ve sıkıştırma gibi ek işlem sonrası işlemlere tabi tutulsa bile, tüm çerçeveler arası sahtekarlıkları tespit etmek için önerilen sistemin performansının iyi olduğunu göstermiştir (22).

Li vd., 2023 çalışmalarında video ekleme sahteciliğini tespit etmek için kamera sensörü desen gürültüsünü kullanmışlardır. Çalışmalarında çerçevenin ön plan nesnelerini çıkartıp ardından referans sensörü desen gürültüsünü ön plan nesneleri olmayan çerçeveler kullanılarak eğitmişlerdir (18).

Ses Tabanlı Sahtecilik

Ses kopyala yapıştır sahteciliği; bir ses kaydındaki herhangi bir bölüm kopyalandıktan sonra aynı ses kaydındaki farklı bir yere eklenmesi ile elde edilen ses sahteciliği çeşididir. Ses kopyala yapıştır sahteciliğinde tek bir ses kaydı üzerinde belirtilen işlemler yapılmaktadır. Ses birleştirme sahteciliği; bir ses dosyasının içine farklı bir ses kaydından bir bölümün eklenmesi ile oluşturulan ses sahteciliği türüdür. Bu sahtecilik türünde ise birden çok ses kaydı bulunmaktadır. Literatürde ses sahteciliği tespiti üzerine yapılan çalışmalar incelendiğinde ses kopyala-yapıştır sahteciliği tespitinin, ses sahtecilik tespitleri arasında en zor problemlerden biri olduğu bilinmektedir (5).

Akdeniz vd., 2022 yılında yaptıkları çalışmada ses kopyala yapıştır sahteciliğini tespit etmek için ilk aşamada ses sinyalini sesli ve sessiz segmentlerine ayırmışlardır. Segmentlerine ayrılan ses sinyalinden her bir segmentten doğrusal öngörü katsayılarını (DÖK) elde etmişlerdir. Her bir ses segmentinden elde ettikleri bu katsayılar arasındaki benzerliği Pearson Korelasyon Katsayısı ile hesaplayarak benzerlik değerine göre sahtecilik işlemi yapılıp yapılmadığına karar vermişlerdir (23).

Moussa vd., 2022 yılında yaptıkları çalışmada ses birleştirme sahteciliğini tespit edebilmek için diziden diziye (Seq2Seq) Transformer ağ yapısını kullanmışlardır (24).

Zhang ve çalışma arkadaşları 2022 yılında yaptıkları çalışmada kodlayıcı-kod çözücü (encoder-decoder) mimarisine dayalı ASLNet isimli ses birleştirme sahteciliğini tespit eden bir yöntem önermişlerdir. Çalışmalarında TIMIT ve FMFCC-A veri kümelerini kullanarak sahte ses verilerini oluşturmuşlardır. Çalışmanın en iyi doğruluk sonuçlarını 99.65% ve 97.40% olarak elde etmişlerdir (25).

Akdeniz vd., 2021 yılında yaptıkları çalışmalarında ses kopyala yapıştır sahteciliğini tespit etmek için ilk aşamada ses sinyalini sesli ve sessiz segmentlerine ayırmışlardır. Segmentlerine ayrılan ses sinyalinden her bir segmentten mel frekansı kepstral katsayılarını (MFCC) ve delta MFCC katsayılarını elde etmişlerdir. Son aşamada ise her bir ses segmentinden elde ettikleri bu özellikler arasındaki benzerliği Pearson Korelasyon Katsayısı ile hesaplayarak benzerlik değerine göre sahtecilik işlemi yapılıp yapılmadığına karar vermişlerdir (9).

Huang vd., 2020 yılında çalışmalarında ses kayıtlarındaki ses etkinliğini algılamak için sinyali segmentlere ayırmışlardır. Ayrılan ses segmentlerinin her birine Ayrık Fourier Dönüşümü uygulayarak frekans ekseninde ki noktaları özellik olarak almışlardır. Bu özellikleri sıralayıp

bitişik segmentleri karşılaştırmışlardır. Böylelikle benzerlikleri hesaplayarak ses kopyala-yapıştır sahteciliğini tespit etmişlerdir (26).

SONUÇLAR VE TARTIŞMA

Bu çalışmada, dijital multimedya verilerinde özellikle kopyala-yapıştır ve birleştirme sahtecilikleri tespitlerinin incelenmesi üzerine yapılan çalışmalara odaklanılmıştır. Manipülasyona uğrayan dijital multimedya verileri özellikle mahkemelerde, resmi makamlarda değerlendirilmeden önce bütünlük doğrulaması gerektirir. Bu veriler üzerinde yapılan sahteciliklerin tespit edilmesi, verilerin bütünlük doğrulaması, gerçekliğinin anlaşılması ve güvenliği açısından oldukça önemlidir. Bu çalışmada son yıllarda yayınlanmış makalelerin ayrıntılı analizine, çeşitli dijital multimedya verileri üzerine yapılmış sahtecilik yöntemlerine ve literatüre olan katkısına yer verilmiştir. Sonuç olarak, çalışmada dijital multimedya sahteciliğinin tespiti alanında yapılan çalışmalar derlenerek kapsamlı bir özet haline getirilmiştir. Literatürde dijital multimedya verileri üzerinde çeşitli sahtecilik işlemleri uygulandığı görülmüştür. Bu sahtecilik türleri dijital multimedya verilerinin anlam bütünlüklerini değiştirmeye de sebep olabileceği için bu sahtecilik türlerinin tespit edilmesi oldukça önemlidir. Bu çalışmayla, dijital multimedya verileri üzerinde yapılan sahtecilik yöntemlerine ve temel kavramlarına ayrıntılı bir genel bakış sağlanmıştır.

Makalenin ilgili çalışmalar kısmında özellikle son yıllar dikkate alınarak 2020 yılından sonraki çalışmalara yer verilmiştir. Bu durum bu alanda yapılan çalışmaların hala güncelliğini koruduğunu göstermektedir. Görüntü ve video alanında yapılan çalışmaların çoğunluğu derin öğrenme tabanlı yaklaşımlardan oluşurken ses çalışmalarında derin öğrenme tabanlı yaklaşımların azlığı dikkat çekmektedir. Bu durum ise ses sahteciliği tespiti alanında yapılacak olan çalışmalara ihtiyacın daha çok olduğunu göstermektedir.

Teşekkür

Bu çalışma 1002 programı kapsamında 121E725 nolu proje ile TÜBİTAK tarafından desteklenmiştir.

13-16 Ekim 2022 tarihleri arasında Antalya Aksu'daki ATGV Sosyal Tesisleri'nde gerçekleştirilmiş olan Uluslararası Katılımlı 17. Adli Tıp Günleri kapsamında SB36 Referans Numarası verilen "Dijital Multimedya Güvenliği" başlıklı bildirimiz değerlendirme kurulu tarafından Sözlü Sunum olarak kabul edilip sunumu yapılmıştır. Sempozyuma makalenin özet kısmı gönderilmiştir.

Finans: *Bu çalışma için hiç bir kurum veya kuruluştan finansal destek alınmamıştır.*

Çıkar çatışması: *Yazarlar çıkar çatışması olmadığını beyan eder.*

KAYNAKLAR

1. Bloomberg J. Digitization, digitalization, and digital transformation: confuse them at your peril. Forbes. 2018.
2. Desai SD, Pudakalakatti NR, Baligar VP. A survey on intelligent security techniques for high-definition multimedia data. Intelligent Techniques in Signal Processing for Multimedia Security. 2017;15–45. https://doi.org/10.1007/978-3-319-44790-2_2
3. Zanardelli M, Guerrini F, Leonardi R, Adami N. Image forgery detection: a survey of recent deep-learning approaches. Multimedia Tools and Applications. 2022;1–46. https://doi.org/10.1007/s11042-022-13797-w
4. Gupta S, Cho S, Kuo CC. J. Current developments and future trends in audio authentication. Ieee Multimedia. 2011;19(1):50–9. https://doi.org/10.1109/MMUL.2011.74
5. Imran M, Ali Z, Bakhsh ST, Akram S. Blind detection of copy-move forgery in digital audio forensics. IEEE Access. 2017;5:12843–55. https://doi.org/10.1109/ACCESS.2017.2717842
6. Kang X, Wei S. Identifying tampered regions using singular value decomposition in digital image forensics. In: 2008 International conference on computer science and software engineering, Vol. 3. IEEE; 2008. pp. 926–30. https://doi.org/10.1109/CSSE.2008.876
7. Khan MK, Zakariah M, Malik H, Choo KK. R. A novel audio forensic data-set for digital multimedia forensics. Australian Journal of Forensic Sciences. 2018;50(5):525–42. https://doi.org/10.1080/00450618.2017.1296186
8. Bourouis S, Alroobaea R, Alharbi AM, Andejany M, Rubaiee S. Recent advances in digital multimedia tampering detection for forensics analysis. Symmetry. 2020;12(11):1811. https://doi.org/10.3390/sym12111811
9. Akdeniz F, Becerikli Y. Detection of copy-move forgery in audio signal with mel frequency and delta-mel frequency kepstrum coefficients. In: 2021 Innovations in Intelligent Systems and Applications Conference (ASYU). IEEE; 2021. pp. 1–6. https://doi.org/10.1109/ASYU52992.2021.9598977
10. Raghavan S. Digital forensic research: current state of the art. CSI Transactions on ICT. 2013;1(1):91–114. https://doi.org/10.1007/s40012-012-0008-7
11. Yerushalmy I, Hel-Or H. Digital image forgery detection based on lens and sensor aberration. Int J Comput Vis. 2011;92:71–91. https://doi.org/10.1007/s11263-010-0403-1
12. Qazi EUH, Zia T, Almorjan A. Deep learning-based digital image forgery detection system. Applied Sciences. 2022;12(6):2851. https://doi.org/10.3390/app12062851
13. Ali SS, Ganapathi II, Vu NS, Ali SD, Saxena N, Werghi N. Image forgery detection using deep learning by recompressing images. Electronics. 2022;11(3):403. https://doi.org/10.3390/electronics11030403

14. Fatima B, Ghafoor A, Ali SS, Riaz MM. FAST, BRIEF and SIFT based image copy-move forgery detection technique. Multimedia Tools and Applications. 2022;1–15. https://doi.org/10.1007/s11042-022-12915-y
15. Rodriguez-Ortega Y, Ballesteros DM, Renza D. Copy-move forgery detection (CMFD) using deep learning for image and video forensics. Journal of Imaging. 2021;7(3):59. https://doi.org/10.3390/jimaging7030059
16. Manjunatha S, Patil MM. Deep learning-based technique for image tamper detection. In: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). IEEE; 2021. pp. 1278–85. https://doi.org/10.1109/ICICV50876.2021.9388471
17. Barad ZJ, Goswami MM. Image forgery detection using deep learning: a survey. In: 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE; 2020. pp. 571–76. https://doi.org/10.1109/ICACCS48705.2020.9074408
18. Li, Q.; Wang, R.; Xu, D. A Video Splicing Forgery Detection and Localization Algorithm Based on Sensor Pattern Noise. Electronics. 2023, 12, 1362.
19. Patel, J., & Sheth, R. (2022). Passive Video Forgery Detection Techniques to Detect Copy Move Tampering Through Feature Comparison and RANSAC. In Cyber Security and Digital Forensics (pp. 161-177). Springer, Singapore. https://doi.org/10.1007/978-981-16-3961-6_15
20. Raskar, P. S., & Shah, S. K. (2021). Real time object-based video forgery detection using YOLO (V2). Forensic Science International, 327, 110979. https://doi.org/10.1016/j.forsciint.2021.110979
21. Shelke, N. A., & Kasana, S. S. (2021). A comprehensive survey on passive techniques for digital video forgery detection. Multimedia Tools and Applications, 80(4), 6247-6310. https://doi.org/10.1007/s11042-020-09974-4
22. Fadl, S., Han, Q., & Li, Q. (2021). CNN spatiotemporal features and fusion for surveillance video forgery detection. Signal Processing: Image Communication, 90, 116066. https://doi.org/10.1016/j.image.2020.116066
23. Akdeniz, F., & Becerikli, Y. (2022, October). Linear Prediction Coefficients based Copy-Move Forgery Detection in Audio Signal. In 2022 6rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). IEEE. https://doi.org/10.1109/ISMSIT56059.2022.9932794
24. Moussa, D., Hirsch, G., & Riess, C. (2022). Towards Unconstrained Audio Splicing Detection and Localization with Neural Networks. arXiv preprint arXiv:2207.14682.
25. Zhang, Z., Zhao, X., & Yi, X. (2022). ASLNet: An EncoderDecoder Architecture for Audio Splicing Detection and Localization. Security and Communication Networks, 2022. https://doi.org/10.1155/2022/8241298
26. Huang, X., Liu, Z., Lu, W., Liu, H., & Xiang, S. (2020). Fast and effective copy-move detection of digital audio based on auto segment. In Digital Forensics and Forensic Investigations: Breakthroughs in Research and Practice (pp. 127-142). IGI Global. https://doi.org/10.4018/978-1-7998-3025-2.ch011