Bireye Ait Verilerden Üretken Ağlar Aracılığı ile Üretilen Sentetik Verilerin Kullanımı

Oğuzhan ERCAN
Yıldız Teknik Üniversitesi
Bilgisayar Mühendisliği Bölümü
oguzhanercancs@gmail.com

***Özet*— Üretken Çekişmeli Ağlar (GANs) [1] 2014 yılında yayınlanmasından itibaren derin öğrenme alanındaki en popüler araştırma alanlarından olmuştur. Ian Goodfellow tarafından yayınlanan GANs günümüzde otonom araçlar, savunma sanayii, Snapchat filtreleri, deepfake, veri arttırma gibi bir çok alanda kullanılmaktadır. Üretken ağlar ile üretilen sentetik veriler ile oluşturulan çeşitli reklam filmleri, regülasyonu bulunmayan piyasalarda mal varlıklarını manipüle edilmek amacıyla popüler insanlara ait üretilen videolar ve uygunsuz içeriklere kişinin yüzünün aktarımı gibi etik olmama ihtimali olan alanlarda da kullanılmaktadır.**

Anahtar Kelimeler: Auto Encoder, Üretken Çekişmeli Ağlar, Deep Fake, AR, Etik, Yapay Öğrenme

I. GİRİŞ

2014 yılında yayımlanan üretken çekişmeli ağlar ve sonrasında enerji tabanlı yapısal tahminleme yapabilen auto encoder ve down-up sampling tabanlı modeller ile günümüzde kişiye ait verilerden sentetik video-frame veriler üretilmeye başlanmıştır. Bu durum insan yüzünün istenilen formatta sunulmasına olanak sağlamış ve dikkatleri üzerine toplamıştır.

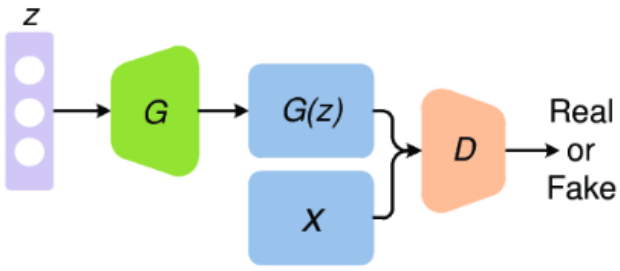
Bahsi geçen gelişmelerden önce ise kişinin tarayıcı geçmişi verileri veya alışveriş sitelerindeki tıklamalarına ait veriler kullanılarak kişiye ait geleceğe dair sentetik veri üretimi gerçeklenmiş ve bu veriler ticari amaçlarca kullanılmıştır. Günümüzde karşımıza cookieler olarak çıkan, kişiye ait verileri kişinin bilgisayarında depolayarak siteye herhangi bir kendini tanıtma işlemi yapmadan dahi bu verileri site yayımcısının kullanıcısına sunan teknolojiler geliştirilmiştir.

Bu veriler ticari, manipülasyon ve şantaj amaçlarıyla kullanılabildiği bir aşamaya gelmiştir. Bu makalede kişiye ait veriler ile üretilen sentetik verilerin çeşitli amaçlar için kullanılması etik ve hukuk açısından inceledim.

II. ÜRETKEN ÇEKIŞMELI AĞLAR

A. İnceleme

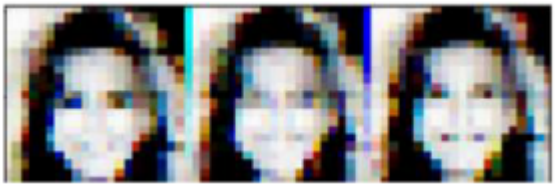
Üretken çekişmeli ağlar doğal veriden sentetik veri üretmeyi hedefleyen bir derin öğrenme modelidir. Uniform bir dağılımı doğal verinin dağılımına yaklaştırarak sentetik verileri doğal verilere benzetir. Üretken (Generative) ve ayırıcı (Discriminator) olarak iki farklı modelin çekişmesi sonucu üretken modelin çıktıları doğal verilere yaklaşır.



Figür 1

Üretken Çekişmeli Ağlar noise olarak adlandırılan uniform vektörü üretken modelde yukarı örnekleyerek doğal verimizin boyutlarına getirir. Ayırıcı model sentetik veri ve doğal veriyi sınıflandırması için kurgulanmıştır. Ayırıcı model doğal ve sentetik veriden gelen giriş değerlerini yapay sinir ağı aracılığıyla doğru şekilde sınıflandıracak şekilde parametrelerini geri yayılım algoritması ile optimize eder. Üretici model ayırıcı modeli kandırmayı hedeflemektedir ve ayırıcı modelden aldığı geri beslemeye göre geri yayılım algoritması ile parametrelerini günceller. Parametreler uniform dağılımını doğal verimizin dağılımına yaklaştırır.

Üretken çekişmeli ağların orijinal makalesinde sunulan implementasyonu[2] gerçekleştirilmesini CELEB A setinde eğittikten sonra elde ettiğim sonuç figür 2'de gösterilmiştir.



Figür 2

B. Üretken Çekişmeli Ağların Diğer Uygulamaları

Üretken çekişmeli ağlar doğal dilden sese, görüntü verisinden videolara, tablo halindeki veriden sosyal verilere

birçok veri türünün sentetik olarak üretilmesinde kullanılmaktadır. Kişisel verilerimiz kullanılarak üretilecek sentetik verilerden en çok dikkat çekenler ise ses ve görüntü verileridir. Bu veriler kullanılarak verinin ait olduğu kişinin gerçekleştirmediği aksiyonlar gerçekleştirilmiş gibi ses veri görüntü verileri üretilebilir.

III. Üretken ağlar kullanilarak üretilen sentetik veri örnekleri

Günümüzde kripto paralar popülaritesini gitgide arttırmaktadır. Bu durumun başrol oyuncularından birisi ise Elon Musk'dır. Çeşitli kripto paraların değerlerini manipüle etmek amacıyla Elon Musk'a ait, konuyla hiçbir ilgisi bulunmayan video verileri kullanılarak onun sesi ve onun görüntüsüymüş gibi üretilen sentetik veriler ile kripto para varlıkları geçtiğimiz 1 yıl boyunca sıkça manipüle edilmiştir.

Rusya-Ukrayna savaşı günümüzdeki sıcak haberlerden biridir. Ukrayna Başkanı Volodimir Zelenski'ye ait, konu ile alakası bulunmayan video verileri kullanılarak Ukrayna'nın savaşı kaybettiğini ve halkın direnişi kesmesini söylediği sentetik veriler üretilmiş ve sosyal medyada paylaşılarak insanları yanıltmak hedeflenmiştir.

Birçok devlet başkanı, şirket yöneticileri, sosyal medya fenomenleri ve sanatçıların verileri kullanılarak üretilen sentetik veriler bu bireyleri takip eden kitleleri çeşitli hedefler için yönlendirmek amacıyla kullanılmaktadır.

IV. Verilerin sentetik olup olmadığının tespiti

Bu sentetik verileri; uzman kişiler derin öğrenme mimarilerini doğru akışta ve yeterli veri ile eğiterek oluşturduğunda biz bireylerin gerçek - sentetik ayrımını yapması mümkün dışı bir hal almaktadır. Yapay öğrenme ile oluşturulan bu sentetik verileri gerçek verilerden ayırt etmek için geliştirilen methodlardan en başarıları gene yapay öğrenme methodlarıdır.

AWS, Facebook, Microsoft ve Partnership on AI's Media Integrity Steering Committee bir araya gelerek Kaggle platformunda Deepfake Detection Challenge: Identify videos with facial or voice manipulations başlığında 1.000.000 dolar değerinde ödüle sahip bir yarışma düzenlemiştir.

Günümüzde üretken ağlar ile üretilen sentetik veriler ile doğal verileri ayırt etmek popülaritesini üstel şekilde arttıran bir araştırma alanıdır. Üretken çekişmeli ağların yapısındaki gibi, sentetik veri üretenler ve bu verilerin sentetik mi doğal veri mi olduğunu tespit edenler arasında büyük bir çekişme vardır.

V. Riza olmadan üretilen sentetik verilerin kullanilmasi

Kişisel verilerin kişinin izni olmadan kullanılması Kişisel Verilerin Kullanımı Kanunu kapsamınca yasaktır. Bu sebeple hukuki olarak kişinin rızası bulunmadan bu verilerin sentetik veri üretmek amacıyla kullanılması uygun değildir.

VI. Rizasi alinan bireylerin verileri kullanilarak üretilen sentetik verilerin kullanilmasi

Kişinin kişisel verilerini kullanmaya izin verdiği taktirde üretken ağlarla sentetik veri üretilmesi KVKK kapsamında incelenmiş bir durum değildir. Üretilen sentetik verinin içeriği ise bu durumun hukuki durumunu belirler. Veriler veri sahibini rencide edecek, haklarını ve özgürlüklerini ihlal edecek veya maddi durumuna zarar verecek şekilde kullanılması hukuki olarak uygun değildir.

Elde edilen kişisel verilere gösterilen rızanın gerçekten rıza olup olmaması da bir diğer sorudur. Kullanıma sunulan uygulamanın çalışması için toplanacak verilere zorunlu olarak izin istemesi hukuki ve etik olarak bir belirsizlik durumudur.[3]

VII. Rizasi alinamayan bireylerin verileri kullanilarak üretilen sentetik verilerin kullanilmasi

Ölmüş, iletişim kurulamayacak durumda olan yada çeşitli hastalıklardan dolayı rızası alınamayacak bireylere ait verilerin sentetik veri üretiminde kullanılması yakın zamanda gündeme gelmiş bir konudur. Ziraat Bankası'nın reklam filminde Kemal Sunal'ın yüzünün kullanılması bu duruma örnektir. Ölmüş olduğu için kendi rızası alınamayan Kemal Sunal'ın mirasçıları ile yapılan sözleşme ile taraflar anlaşmış ve Kemal Sunal'a ait veriler kullanılarak reklam filmi üretilmiştir.

Türk Medeni Kanunu incelendiğinde hukuki açıdan bahsi geçen sözleşmenin yapılması uygun değildir. Kişinin benliğine ait, sıkı sıkıya bağlanmış haklar; bu bağlamda kişisel verilerin hakları bireyin ölümü ile beraber bireyin kişiliği sona erdiği kabul edilir ve mirasçılar tarafından herhangi bir hak talebinde bulunamaz.[4]

Türk Medeni Kanunu'nda kişinin hak ehliyetini kaybetmesinin kişiliğinin korunmasını da kaybettiği anlamına gelip gelmediği hususunda bir açıklık bulunmamaktadır. Bu konuda herhangi bir düzenleme bulunmaması bu verilerin kullanımı hakkında soru işaretleri bırakmaktadır.

Hatırayı Koruma Doktrini kişinin ölümü ile beraber kişisel veriler üzerinde hak ve ehliyetinin sona erdiğini savunur. Bu konudaki dayanak noktası ise kişinin ölümünden

sonra kişisel haklarına yapılan saldırılar için herhangi bir savunma yapamayacak oluşudur.

Hatırayı Koruma Doktrini kişinin ölümünden sonra hakların savunması konusunda kişiyi tamamen savunmasız bırakmamıştır. Ölen kişinin haklarına yapılan saldırı kişinin mirasçılarına yapılmış olarak görülürse kişinin mirasçılarının bu saldırıları savunmak için dava açabileceğini öne sürer.

VIII. Üretilen Sentetik Verilerin Toplum Üzerine Etkisi

Sentetik veri üretimi için kullanılan kişisel verilerin topluma mal olmuş kişilere ait olması; üretilen sentetik verilerin içeriğine bağlı olarak toplumu çeşitli şekillerde etkileyebilir.

Finansal piyasaları manipüle etmek amacıyla piyasada söz sahibi kişilere ait sentetik verilerin oluşturulması bireylerin maddi olarak zarara uğramasına sebep olabilir. Bu durum hukuki ve etik açıdan uygun değildir.

Savaş, siyaset, ekonomik krizler ve pandemi gibi toplumsal yaşamı doğrudan etkileyen alanlarda söz sahibi kişilere ait sentetik veri üretilmesi toplum yaşamında ortaya anarşizm, yağmalama, sağlık sektörünün sekteye uğraması gibi problemlere yol açabilir.

Topluma mal olmuş, eserleri toplumca değer olarak kabul edilmiş kişilere ait verilerden üretilen sentetik verilerin veri sahibini rencide etmesi, haklarına saldırması vb. durumlar toplum değerlerine yapılmış bir saldırı niteliği taşır ve uluslararası ilişkilerde problemlere yol açabilir.

IX. Sonuç

Sentetik veriler eğlence sektöründen sağlık uygulamalarına çok geniş bir yelpazede toplum yararına kullanılmaktadır. Fakat üretilen sentetik verilerde art niyet bulunması birey ve toplum sağlığını korumak adına etik ve hukuki olarak kabul edilemez durumlara yol açabilmektedir.

X. Referanslar

1. I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio. Generative adversarial nets. In Advances in neural information processing systems, pages 2672–2680, 2014
2. https://github.com/Oguzhanercan/GANs/blob/master/tutorial/GANs_English/VanillaGANs.ipynb
3. https://dergipark.org.tr/en/download/article-file/1517493
4. https://dergipark.org.tr/en/download/article-file/15174