OPUS
Uluslararası Toplum Araştırmaları Dergisi
International Journal of Society Researches

ISSN:2528-9527
E-ISSN : 2528-9535
Yıl *Year* : 10
Cilt *Volume*:16
Sayı *Issue* :28
Ağustos *August* 2020
Makalenin Geliş Tarihi *Received Date*: 03/02/2020
Makalenin Kabul Tarihi *Accepted Date*: 27/07/2020

Dijital Çağın Yeni Tehlikesi "Deepfake"

DOI: 10.26466/opus.683819

*

Mustafa Evren Berk *
* Dr. Öğr.Üyesi, Necmettin Erbakan Üniversitesi, Güzel Sanatlar Fakültesi Sinema-TV
E-Posta: meberk@erbakan.edu.tr **ORCID:** 0000-0002-5395-6204

Öz

Bilgisayarların icat edilmesiyle hayatımız her alanda kolaylaşmış, bir o kadar da tehlikenin içine girmiştir. İnsanoğlu bilgisayarları günümüze kadar gündelik hayatlarını kolaylaştırmak için evlerinin içine sokmuştur. Ancak yeni yazılım dilleri ve teknolojinin ilerlemesiyle bilgisayar isteğimiz dışında olsa bile insanları tehlikeye sokmaktadır. Bunlardan bir tanesi de 2017 yılında duyduğumuz derin sahte diğer orijinal adıyla Deepfake'tir. Makalemizin konusu da son zamanlarda kamuoyunu meşgul eden ve insanların aslında söylemedikleri halde söylenmiş gibi gösteren yüz ifadelerinin insanları ne tür çıkmaza soktuklarını göstermektir. Siyaset ya da sanat alanında tanınmış insanların yüzlerini başka yüzlere yerleştirme yoluyla yapılan bu işlem gelecekte insanların özel hayatlarını daha çok tehdit etmeye başlayacaktır. Bu konu sadece ünlü insanlar için değil herhangi bir kişi için de geçerlidir. Deepfake konusu ilerleyen zamanlarda teknolojinin de yardımı ile kendini çok geliştirerek hem kullanıcıların kullanımı açısından kolaylaşacak hem de uygunsuz video kirliliği ortaya çıkacaktır. Bu araştırma, Deepfake konusunda ülkemizde sıkıntı çeken kişilerin ne yapmaları gerektiği konusunda yol göstermek için de önemlidir. Makalede doküman analizi yapılmış olup, Deepfake tehlikesinin hem kötü hem de iyi yönleriyle tartışılarak, ne gibi önlemler alınabileceği hakkında da bilgi vermektedir. Deepfake konusunu bu açıdan diğer çalışmalara yön vermesi bakımından da önemlidir. Araştırmada deepfake videoları yüzünden birçok insanın sıkıntıya düştüğü ve bu videoların ilk başta intikam amaçlı olarak yapıldığı daha sonraları da eğlenceye yönelik içeriklerin üretildiği görülmüştür.

Anahtar Kelimeler: *Derin Sahte, Derin Öğrenme, Yapay Zeka*

OPUS
Uluslararası Toplum Araştırmaları Dergisi
International Journal of Society Researches

ISSN:2528-9527
E-ISSN : 2528-9535
Yıl *Year* : 10
Cilt *Volume*:16
Sayı *Issue* :28
Ağustos *August* 2020
Makalenin Geliş Tarihi *Received Date*: 03/02/2020
Makalenin Kabul Tarihi *Accepted Date*: 27/07/2020

The New Threat Of The Digital Age "Deepfake"

*

Abstract

With the invention of computers, our life has become easier in every area and has been in danger. Human beings have put computers in their homes to make their daily lives easier. However, with the advancement of new software languages and technology, even if the computer is out of our desire, it puts people at risk. One of them is Deepfake, which is another deep fake we heard in 2017. The subject of our article is to show what kind of deadlock people's facial expressions have recently been busy with and that make people seem to have been told even though they don't actually say it. This process, which is done by placing the faces of well-known people in the field of politics or art, will start to threaten the private lives of people more in the future. This topic applies not only to famous people, but also to any person. The subject of Deepfake will improve itself with the help of technology in the future and it will both be easier for users to use and inappropriate video pollution will occur. This research is also important to guide the people who have trouble in our country about Deepfake about what to do. The article has been examined with the literature review method and also gives information about what measures can be taken by discussing the danger of Deepfake with both its bad and good aspects. Deepfake is also important in terms of guiding other studies in this respect. In the research, it was seen that many people were distressed because of the deepfake videos and these videos were made for revenge at first and then entertainment content was produced.

Keywords: *Deepfake Deep Learning, Artificial İntelligence*

Giriş

Bilgisayarların icat edilmesiyle başlayan dijital yolculuğun günümüze gelene kadar bu denli bir değişime uğrayacağı şüphesiz insanoğlunun aklından geçmemiştir. Yine bu insanoğlunun bitmeyen istekleri ve hayalleri sayesinde bilgisayarlar kullanımı, insanların hayal edemedikleri bir ortam oluşturmuştur. İnsanların istekleri ve hayalleriyle şekillenen teknolojiler gün geçtikçe insanları tüketim yoluna teşvik ederken bir taraftan da insanların zevk aldıkları konularda ihtiyaçları oluşturanlarla karşılıklı ilişki içerisinde olmalarına sebep olmuştur. Teknolojiler insanların hayatlarını kolaylaştırırken, bir takım kötü emeller için de kullanılmaktadır. İnsanoğlu bilgisayar teknolojisini 2000'li yıllara kadar kendi çalışma alanlarında kullanmak için amaçlamışlarsa da, gelişen ve globalleşen siber dünyada oluşturulan trendler sayesinde bu amaçlar farklı alanlara kaymıştır.

2000'li yıllardan sonra artan sosyal video paylaşım platformları sayesinde insanlar, eğlence ya da bilgi vermek amacıyla videolar çekip, bunları video paylaşım platfromlarına yüklemiştir. İnsanlar yüklenen içeriklere göre de gelir kazanmaya başlamasıyla birlikte bu eğlence sektörü ticari bir alana dönüşmüştür. Ancak oluşturulan video içeriklerin denetiminin de yapılması ayrı bir sorun teşkil etmektedir. Yazılımların oluşturulması ile birlikte videolarda yapılan manipülasyonlar, kimisi için eğlence konusu olurken, videoda bahsi geçen şahıs ya da kurumlar için de rahatsız edici hale gelmiştir.

Makalemizin konusunu oluşturan sorunlu durumlardan bir tanesi de son zamanlarda sosyal paylaşımlar platformlarında sıklıkla gördüğümüz ünlü oyuncuların ya da politkacıların "deepfake" (Derin Sahte) adı verilen uygulama ile yapılan yüz ifadelerindeki video manipülasyon işlemidir. Bu işlemde deepfake yapılması istenilen herhangi bir ünlü politikacının yüzünü, başka bir insanın yüzündeki ifadeleri referans alınarak, o politikacının yüzüne monte edilmektedir.

Çalışmada, doküman analizi yapılmış olup konuyla ilgili kaynaklar taranmış ve değerlendirme yapılmıştır. Konu hakkında daha önceden yapılmış çok fazla araştırma olmaması, çalışmanın da önemini vurgulamaktadır. Araştırmada deepfake videoların başlangıç zamanı ve nasıl geliştiği ile ilgili makaleler ve haberler incelenerek konu ile ilgili doküman analizi yapılmıştır. Farklı başlıklarda Deepfake teknolojisinin geleceği hakkında bilgi verilmiştir buna istinaden gelecekte insanları ne gibi tehlikelerin beklediği ve ayrıca kişi

hakları, özel hayatın gizliliği gibi kanuni hakların nasıl kullanılabileceği konusunda da bilgi verilmiştir.

Sonuç kısmında deepfake teknolojisinin şimdi ve ileriki zamanlarda sosyal, politik anlamlarda ne derece tehlikeli olabileceğinin farkındalığını yaratmak konusu bakımından önemlidir. Yüklenen videoların kontrolü hakkında yeni tartışmalar açacaktır. Bununla ilgili hangi önlemlerin alınabileceği hakkında bilgi verilecektir.

Deepfake nedir?

Deepfake, bir kişinin, surat ifadelerini gelişmiş bir yazılım kullanılarak görsel ve sesli içerik olarak manipüle edilme işlemi olarak tanımlanabilir. Deepfakes, daha çok görsel-işitsel manipülasyonun bir bileşenidir. Görsel-işitsel manipülasyon, medyanın yorumunu etkilemek için herhangi bir sosyoteknik araçtır.(Paris ve diğerleri, 2018, s.1). Deepfake, bir yüz ifadesinin başka bir yüz ifadesine belli bir amaç doğrultusunda eklenmesi işlemidir (Nguyen ve diğerleri, 2019, s.1).

Deep fake, gerçek insanların video ve ses kayıtlarına yüzler ve sesler eklemek için makine öğrenme algoritmalarından yararlanır ve gerçekçi taklitlerin yaratılmasını sağlar. Daha basit ifade etmek gerekirse, teknoloji "ses yaratmayı mümkün kılar ve gerçek insanların asla söylemedikleri veya yapmadığı şeyleri söyleyip yaptıkları videolardır (Siekierski, 2019, s.1).

Deepfake'in ilk geliştiricisinin bir yazılım mühendisi olduğunu belirtmek önemlidir. Ancak, deepfake yazılımının yaratılmasında kullanılan Google ve NVidia gibi yazılım şirketlerinin açık kaynaklı olmasının da payı büyüktür. Geliştirme süreci, hesaplama parametreleri ve algoritmaları hakkında teknik bir bilgi birikimine ihtiyaç duyulmaktadır (Gardiner, 2019, s.8).

İnsanları ve olayları yanlış tanıtan videolar ve diğer içerikler oluşturmak için kullanılabilecek çeşitli teknikler vardır. Deepfake'in yaratıcısı, reddit adlı websitede yine kendi kullanıcı adını kullanarak kamuoyunun dikkatini çekmiştir. Bu teknoloji, yapay zekayı kullanarak derin öğrenme tekniğiyle video ve resimlerden insan yüzlerini tanımaktadır. Bu teknik, manipüle edilecek karakterin yüzünün birçok video ya da resimlerini yapay zeka dayalı algoritmalara analiz edip, bu algoritmaların çıkardıkları sonuçlara göre yüzünün değişmesini istenilen kişi üstünde manipüle edilmektedir. Bu teknik ile şahısların resimlerinin kullanım haklarına sahip olmadan, bir arkadaşınızın yüz

görüntülerini kullanarak yetişkin içerik üretmesine de sebep olabilmektedir (Dodge ve diğerleri, 2018, s.1). Ünlü sanatçıların ve politikacıların gündemde olmasından dolayı internette video ve fotoğrafların çokluğu deepfake için potansiyel hedef olarak görülmektedir (Nguyen, 2019).

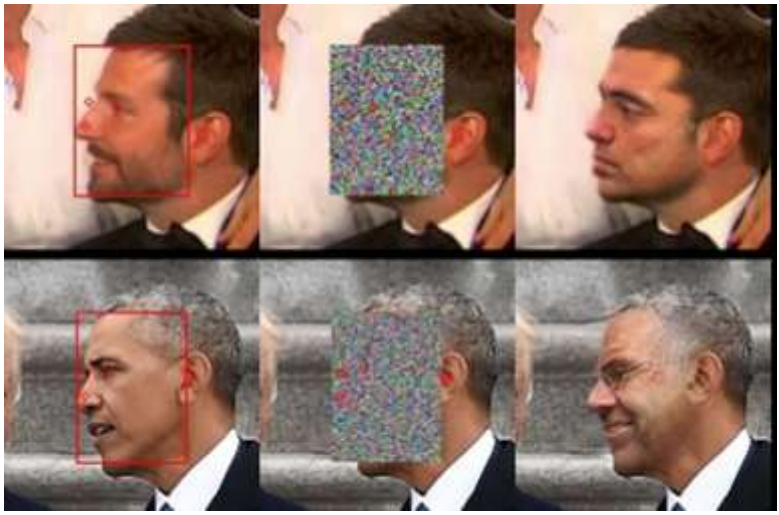
Deepfake içerikli videolardan daha çok ünlü ve saygın kişiler etkilenmiştir. Ayrıca son dönemlerde bunlardan en çok siyasiler nasibini almıştır. Barack Obama, Donald Trump gibi önemli siyasetçiler deepfake kullanıcıları tarafından dalga konusu olmuşlardır. Aynı şekilde hollywood'un ünlü artist ve aktrisleri de deepfake'in mağduru olmuşlardır. Kendilerini yetişkin içerikli filmlerin içerisinde bulmuşlardır.

Deepfake terimi, ilk kez 2017 yılında reddit adlı web sitesinde yine sitenin deepfake kullanıcısı tarafından oluşturulan ünlülerin yetişkin içerikli uygunsuz videolarını yayınlamasıyla ortaya çıkmıştır. Daha sonra reddit paylaşım sitesi bu içeriklerden dolayı odak noktası olmuştur. Deepfake sisteminin bilinen 3 tür kullanımı vardır;

Yüz değiştirme: Yüz yerleştirme olarak da bilinen yüz değiştirme, yüzü değiştirilecek hedef insanın fotoğraflarının, başka bir kişiyi video manipülasyon tekniği ile monte edilmesidir. Buradaki amaç yüz değiştirmesi yapılacak olan insanın yüzünden olabildiğince kalitesi yüksek resim ya da videoların seçilip, yine seçilen bu materyallerden yazılım, kaynak yüzden hedef yüze yapay zeka sistemiyle resimlerin monte edilmesi işlemidir.

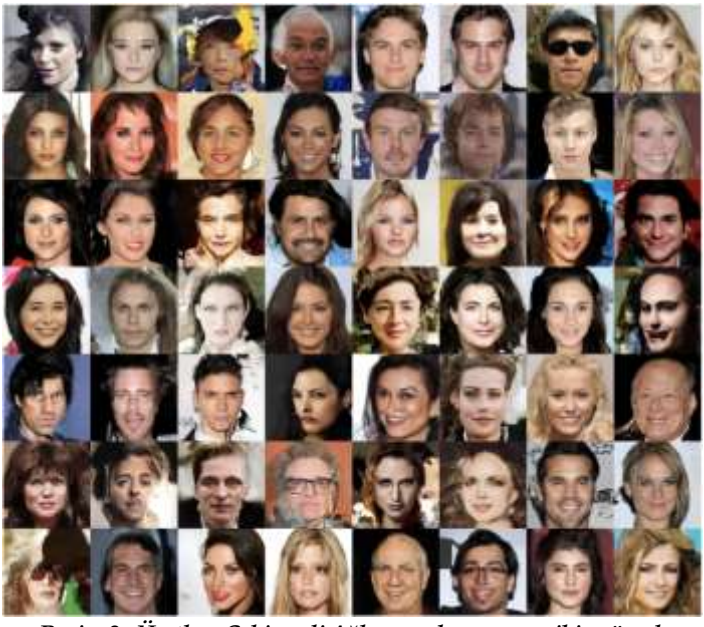
Resim 1. Yüz değiştirme tekniğine örnek bir görsel

İfade değiştirme: Kuklacılık olarak da bilinen yüz yeniden canlandırma, bir hedefin yüzünün özelliklerini, hareketleri dahil, ağız, kaş, göz ve ifadelerin tekrar yaratılması işlemidir. İfade değiştirme tekniği, kaynak videodan alınan yüz hareketlerinin başka bir kişinin yüz videosunun üzerine eklenmesi işlemidir. Bu işlem aslında hedef kişinin o bir konu hakkında bir şey söylemese bile, kaynak videodan aldığı ifadelerin taklit edilmesi işlemidir.



Resim 2. Deepfake Yazılımlarının işleyiş mantığına bir örnek

Yüz yaratımı: Generative Adversarial Networks, (Üretken Çekişmeli Ağlar) tarafından geliştirilen bu sistemle iki farklı sinir ağı oluşturulmaktadır. Bunlarda üretken ve ayrıştırıcı olmak üzere iki ayrılmıştır. Her ikisi de birbirleriyle mücadele içerisindedir. Mücadele etmelerindeki amaç, üretken ağı resim oluştururken ayrıştırıcı ağ ise bu resmin gerçek olup olmadığı hakkında derin öğrenme sürecine girerler. Eğer üretken kısım ayrıştırıcıyı kandırırsa, ayrıştırıcı resmin gerçekliği hakkında derin öğrenmeye geçiyor. Ayrıştırıcı üretkenin ortaya çıkardığı sonucu sahte olarak anlarsa bu sefer üretken daha gerçekçi yani sahte olunmadığını anlayacak şekilde üretmeye devam ediyor (Farid ve diğerleri, 2019, s.4).



Resim 3. Üretken Çekişmeli Ağların çalışma prensibine örnek

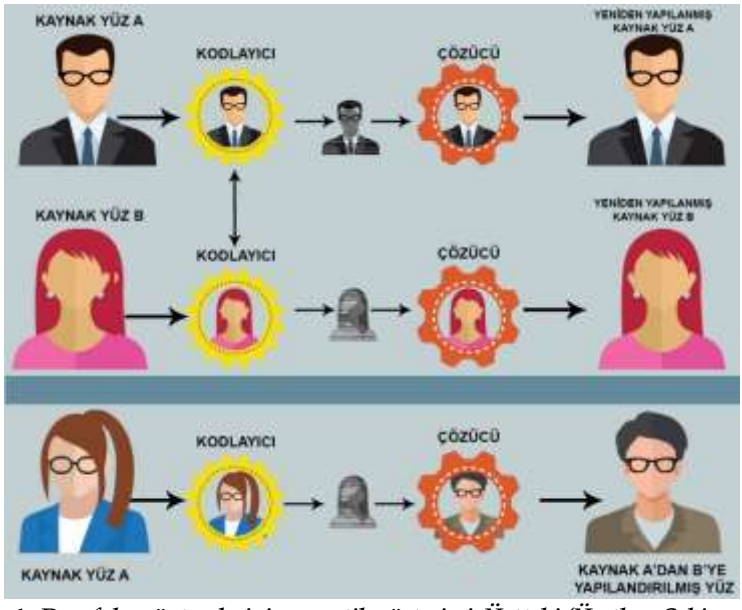
Her üç yöntemin de kendine özgü çalışma prensipleri vardır. En çok tercih edilen ve kullanılan teknik yüz değiştirme (Face Replacement) işlemidir. Bu işlem çok zaman alabilmektedir. Bilgisayarın özelliklerine ve hızına göre bu işlem uzayıp kısalabilmektedir. Ancak kısa sürede sonuç almak adına donanım olarak güçlü bir bilgisayar hesaplamaları kısa sürede yapılmasına imkan tanıyacaktır. İşlemlerin yapılabilmesi için CUDA destekli ekran kartının CPU işlemcilere göre daha verimli olduğu, deepfake programının kurucuları tarafından da desteklenmiş olup ona göre bazı kaynakların indirilmesi için kendi sitelerinde bunları paylaşmışlardır. Görsel manipülasyon bilgisayar teknolojisinin çıkması ve yazılım sektörünün de etkisiyle beraber çok önceleri yapılmaktadır. Bu manipülasyonlar tek kare görüntü olarak yapılmıştır. Görsel efektlerin kullanılmasıyla birlikte bu işlem hareketli görüntülerde de yapılmaktadır fakat bunun için bu alanda çalışıyor olmak ya da bu işin uzmanı olmak gerekmektedir. Ancak Deepfake çıktıktan sonra gerekli yazılım ve yönergelerle bu işi herkesin yapabileceği hale getirmişlerdir. Derin öğrenme adı

altında işlem yapan yazılımlar, bu yüz değiştirme işlemini çeşitli algoritmaların hesaplanması ile birlikte daha kolay ve hızlı hale dönüşmüştür. Deepfake genel olarak üç işlemden geçmektedir.

Çıkarma: Çıkarma işleminde kaynak ve hedef video ya da resim dosyalarının yazılımın algoritmalar sayesinde yüzleri tanıyıp sadece o alanı resim olarak algılama yöntemidir. Bu yöntem sayesinde yazılım, kaynak yüzden aldığı verileri hedef yüze yerleştirmesine imkan tanıyan bir işlemi hazırlamaktadır. Çıkarma işleminde kaynak video ya da resimlerden çıkartılan yüz resimleri, derin öğrenme aşaması için kaynak olarak kullanılmaktadır.

Öğrenme: Hedef ve kaynak dosyadan çıkarılan resimler autoencoder işlemi (oto kodlayıcı) adı verilen derin öğrenme sürecine girmektedirler. Bu süreçte iki sinir ağı kullanılmaktadır. Bir tanesi kaynak yüz için diğeri ise hedef yüz için. İki sinir ağı da aynı encoder (kodlayıcı)'ı kullanırken, ayrıca iki farklı çözücü de kullanmaktadırlar. Bunun nedeni iki yüz de benzer temel mimariye sahip olduğu içindir. Her iki sinir ağın da derin öğrenmesi otomatik kodlama işlemini, benzer bir yüzün görüntüsünü, orijinal sürümüne yeniden yapılandırana kadar devam ettirir.

Son aşama (Oluşturma): Son aşama olarak adlandırılan işlem, derin öğrenme sürecinde yazılımın kaynak ve hedef yüzlerin yer değişimini yapmasında kullandığı algoritmalar doğrultusunda yüz değiştirme işlemi gerçekleşmektedir. Yazılım her ne kadar programlandığı şekilde algoritmaları kullanarak işlem yapsa da kusursuz bir yüz değiştirme işlemi yapması beklenmemektedir. Bu tamamen kaynak dosyaların çokluğuna ya da kalitesine bağlı olarak değişmektedir. Bu aşamada yazılım derin öğrenme sürecinde kullandığı kaynak resim ya da video dosyalarından çıkardığı resimleri hedef yüze eşleştirme için programlanmıştır. Bu aşamaya gelmeden önce kaynak karakterin yüz ifadeleri ne kadar çok olursa yüz eşleştirmesi de o derece kaliteli sonuç verecektir. (Farid ve diğerleri, 2019, s.4).



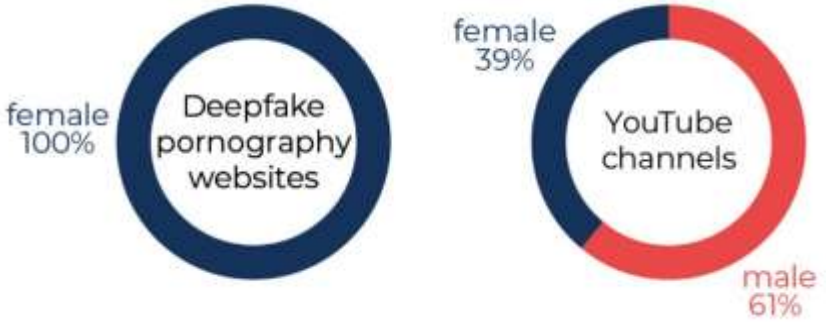
Resim 4. Deepfake yöntemlerinin şematik gösterimi. Üstteki (Üretken Çekişmeli Ağlar) gösterimin için örnektir. Alttaki görünüm ise yaygın olarak kullanılan yüz değiştirmeye örnektir.

Deepfake kullanımı tehdit olarak görülebilir mi?

Deepfake kullanımı, ilk başlarda yetişkin içeriklerle ön plana çıkmış olsa da insan zekasının farklı alanlara yönelmesiyle deepfake'i daha tehlikeli olan siyasi platforma taşıması, konuyu bambaşka bir yöne süreklemiştir. Barack Obama, Viladamir Puttin, Donald Trump gibi devlet başkanlarının konuşmalarının değiştirilmesi ve bunların kötü yönde kullanımı tehlikenin ne boyutta olduğunda bize fikir vermektedir. Ünlü sanatçılar kendilerinin rızası olmadan uygunsuz deepfake videolarında görülmektedir. Birçok sanatçı yasal olarak bir savaş başlatmışlardır. Hatta insanlar sosyal paylaşım sitelerinin yorumlarında, kendi eski kız arkadaşlarına dahi deepfake'i uygunsuz amaçlı kullanmak için sosyal paylaşım sitelerinden bu işlemin nasıl yapılacağı hakkında yardım almaktadırlar.

Deeptrace'in araştırmasına göre deepfake kullanımı, uygunsuz sitelerde sadece bayanlar üzerinde %100 kullanılırken, Youtube videolarında ise bu

oran erkeklerde % 61, bayanlarda ise %39 olduğu görülmüştür. (www.spectrum.ieee.org , 2019).



Resim 5. Deepfake kullanım sıklığı hakkında yapılan araştırma sonucu

2016 Amerikan seçimlerinin ardından Amerika Birleşik Devletleri Başkanı Trump, fake news (yalan haber) hakkında bilgi vermesinin ardından tüm sosyal medya platformlarında bu türden haberlerle mücadele etmesi gündemin konusu olmuştur. Deepfake yazılımlarının yapay zeka kullanarak yaptıkları bu videolardan nasibini alan da Donald Trump olmuştur. Sosyal video paylaşım sitelerinde yayınlanan Amerika Birleşik devletleri eski başkanı Barack Obama'nın deepfake videosunda, " Başkan Trump tam bir ahmak" cümlesi, sanki onun ağzından çıkmış gibi gösterilmesi bütün dünyada yankı yaratmıştır. Bu yankı deepfake'in ne kadar güçlü bir manipülasyon yaratma aracı olduğunu açıkça göstermiştir.

2020 yılında gerçekleşecek olan Amerika seçimleri öncesinde deepfake videolarının, Dezenformasyon ve 2020 seçimleri raporuna göre seçmenleri yanıltabileceği vurgulanmıştır. İnsanlar önceleri gördüğüme inanırım fikrini savunurken, artık neyin gerçek ya da sahte olduğunun çelişkisi içindedirler. Bu sebeple deepfake teknolojisi tüm dünyada dengeleri değiştirebilecek bir konuma gelecektir. Yakın zamanda seslerin klonlaması işlemi de başarıyla gerçekleşmiştir. Bu işlem; klonmasını istediğiniz bir insanın sesini, yazılıma yükleterek taranması sağlanmaktadır. Yazılım kaynak sesi taradıktan sonra, istenilen konuşma yazısının yazılıma girilerek, kaynak sesin ağzından çıkıyormuş gibi çıktı olarak sunmaktadır.

Resim 6. BuzzFeed tarafından yayınlanan deepfake videosu. Sağ taraftaki aktör Jordan Peele'in dudak hareketleri ve konuşması sol taraftaki Barack Obama'ya monte edilmiş hali

Deepfake'in ilk çıkış amacı kötü amaçlı olsa da, sosyal medyada eğlence amaçlı için de kullanıldığı sosyal medyalara yüklenen videolardan görülmektedir. Sosyal paylaşım sitelerindeki örneklerde genellikle ölen bay ya da bayan sinema sanatçılarının yüzleri başka bir karakterin yüzüne monte edilmektedir. Ayrıca sadece ölen değil, eğlence amaçlı da ünlü siyasetçiler ya da oyuncuların yüzleri başka bir insanın yüzüne yerleştirilmektedir. Deepfake'in diğer bir kullanım alanı olarak sinemada üç boyutlu olarak yüksek maliyetle yapılan bu türden yüz değiştirme işlemlerinin yerini alacağı düşünülmektedir. Ölen sinema sanatçıların yüzleri başka kaynak insanlara aktarılarak yine kaynak insanın konuşma ve yüz ifadelerini kullanılması sonucu bu türden maliyetli yapımların daha az maliyetli ve hızlı sonuç çıkması açısından deepfake kullanımı amacının dışında da olsa istenilen alanda kendine yer edinecektir.

Resim 7. Star Wars Rouge One filminden bir kare üstteki orijinal sahne alttaki deepfake uygulanmış Prenses Leia karakteri)

Derin fake teknolojisi, eğitimciler için öğrencilere okumalar ya da dersler gibi geleneksel araçlara göre ilgi çekici şekillerde bilgi sağlama yeteneği de dahil olmak üzere bir dizi fırsat yaratmaktadır. Bu, sıradan videoya erişimi artırarak mümkün olan daha önceki bir eğitim yeniliği dalgasına benzemektedir. Örneğin doğrudan öğrencilere konuşan tarihi bir figürün videolarını üretmek mümkün olacaktır.(Citron ve diğerleri., 2018, s.14).

Sonuç

Deepfake videolarının sayısı her geçen gün artmakta buna bağlı olarak ortaya çıkan yalan yanlış haberlerin de sayısı çoğalmaktadır. Hangi haberin doğru ya da yanlış olduğunu fark edemeyecek kadar kaliteli sonuçlar ortaya çıkmaktadır. İnsanlar bu türden videolarının doğruluğunun ispatının gerçek kaynak sahiplerinden duyana ya da görene kadar bir kaos ve kaygı içerisindedirler. Ayrıca yeni deepfake yazılımlarının ortaya çıkmasıyla, kimisi için tehlike gibi gözüken kimisi için de eğlence amaçlı olan bu yazılımlar akıllı cep telefonlarına kadar düşmüştür. Yazılım her şey belli bir sıralamaya göre otomatik olarak yapmaktadır. Kullanıcıya sadece gerekli resimleri bulmak kalmıştır.

Amerika seçimlerinin yaklaşmasıyla beraber deepfake'in bir korku unsuru olduğu bazı sosyal medya paylaşım sitelerinde yasaklanması bu durumu ortaya koymaktadır. Deepfake'in ileriki zamanlarda görsel propaganda aracı olarak kullanılabileceği, yapılan videolardan da anlaşılmaktadır. Deepfake videolarından sonra akıllara genel bir soru geliyor. Kaynağına güvenmediğimiz bir videoya artık güvenebilir miyiz? Bu sorudan sonuca çıkmak gerekirse video ile ilişkili tüm karakterlerin başı ağrıyacaktır. Deepfake ile oluşturulan video ile ilgili herkes kendini temize çıkarmak için uğraşacak ya da hukuksal açıdan mücadele edecektir. Peki bu videoların yüklenmesini engelleyecek bir sistem oluşturulacak mıdır? Şu ana kadar video sosyal paylaşım sitelerinden sayısız deepfake videoları görüntülenmektedir. Birçoğunun da karakter sahibinden izin alınmadığını düşünülürse, bu video kirliliği nereye kadar devam edecektir.

Yazılım sahipleri deepfake yazılımlarının gelişmiş versiyonlarını piyasaya sürmeye devam edecektir. Yazılımlar genellikle gelen taleplere göre şekillenmektedir. Bir sonraki yazılım sadece instagram, facebook ya da kişisel fotoğraflarınıza erişim imkanı sağlayan bir algoritma oluşturarak sizin deep-

fake videosu yapmak için araştırdığınız fotoğraf kütüphanenizi çok kısa sürede kendisi otomatik olarak kaydedecektir. Bu yüzden sahip olunan sosyal paylaşım sitelerindeki ayarlarınızı güncellemeniz gerekecektir.

İnsanların internette paylaştıkları resim ya da videolardan yapılan deepfake videoları uygunsuz içerik olarak internete yüklenme imkanları oluşacaktır. Daha kötüsü sırf paylaşıma izin verilen videolar yüzünden de saldırısı yapılan kişiden para talebinde bulunabilirler.

Peki bu durumlara düşmemek için ne yapmak gerekir? Daha doğrusu bu türden saldırılardan uzak durmak için kullanıcının ne yapması gerekmektedir? Teknolojinin insan işlerini kolaylaştıran bir araç olduğu aşikârdır ancak yazılım sektörü ve insanların eğlence anlayışlarının değişmesi yaratıcılık konusunda ne tür bir çıkmaza girdiğimizin de bir göstergesidir. İnsanların "nasıl olsa ben ünlü biri değilim benim deepfake videom ile uğraşmazlar" düşüncesine girmesi şu şartlar altında yanlış bir düşünce olacaktır. Çünkü eski sevgiliniz sizden intikam almak için bu türden uygunsuz işlere başvurabilir. Yüzünüz artık sizin yüzünüz değildir. Bu yüzden paylaşım sitelerinden şahsi resimlerimizi paylaşırken tekrar düşünmemiz gerekmektedir.

Sosyal paylaşım sitelerine video yüklerken, paylaşım site sahipleri her yüklenen içerik için bir karekod uygulaması oluşturabilir. Böylelikle o videonun kontrol edildikten sonra yüklendiğine dair bir bilgi içerebilir. Ünlü devlet adamlarının ve siyasetçilerin kaos oluşturacak deepfake videolarının denetimi, yine devlet tarafından oluşturulan karekod tanıyan yazılım sayesinde, bu videoyu izlemek isteyen kullanıcının kendi telefonuyla videodaki karekodunu okutarak izlediği videonun gerçek ya da sahte bir haber olup olmadığını bu sistemle öğrenilebilir.

Böyle bir durumla karşılaşan vatandaşların ilk olarak Savcılığa suç duyurusunda bulunmaları gerekmektedir. Savcılık araştırma sonucu deepfake videolarını yapan suçluların IP numaralarından yer tespiti yapılıp haklarında TCK 134. maddesinde özel hayatın gizliliğini ihlal , TCK 136. Maddesinde kişisel verileri ele geçirme ve TCK 125. maddesinde hakaret suçlarından dava açılabilir. Deepfake yazılımlarının her geçen gün hızla yayılmasıyla birlikte, yapılan videolardan insanların bu türden eğlence ya da uygunsuz içerik üretmek için başvurdukları yazılımlar her geçen gün kendini geliştirerek insanların hayatlarını kabusa çevirecektir. Özel hayatın gizliliği bu nedenle çok önemli bir konudur. Bu konuda sosyal paylaşım sitelerine üye olanların bu konuya dikkat etmeleri gerekmektedir.

EXTENDED ABSTRACT

The New Threat Of The Dıgıtal Age "Deepfake"

*
Mustafa Evren Berk
Necmettin Erbakan University

Undoubtedly, the digital journey that started with the invention of computers has undergone such a change until today. Again, thanks to the endless wishes and dreams of this human being, the use of computers has created an environment that people cannot imagine. While the technologies shaped by people's desires and dreams are increasingly encouraging people to the way of consumption, they have also been in a mutual relationship with the people who create the needs in the subjects they enjoy. While technologies make people's lives easier, they are also used for a number of bad goals. Although human beings aimed to use computer technology in their own work areas until 2000s, these goals have shifted to different fields thanks to the trends created in the developing and globalizing cyber world.

Thanks to the increasing social video sharing platforms after 2000s, people took videos and uploaded them to video sharing platforms for entertainment or information. As people started to earn income based on the content uploaded, this entertainment industry has turned into a commercial space. However, controlling the created video contents also constitutes a separate problem. With the creation of software, manipulations in videos have become a subject of entertainment for some, but have become disturbing for the individuals or institutions mentioned in the video.

One of the problematic issues that constitute the subject of our article is the video manipulation process of facial expressions of famous actors or politicians, who we have frequently seen on social networks, with the application called "deepfake". In this process, the face of any famous politician who is wanted to be deepfake is mounted on the face of that politician by taking the expressions on the face of another person.

In the study, document analysis has been done, related resources have been scanned and evaluated. The lack of much previous research on the topic emphasizes the importance of the study. In the research, articles and news related to the start time of the deepfake videos and how they evolved were analyzed and a document analysis was made on the subject. Information on

the future of Deepfake technology has been given under different headings. In addition, information was given on what dangers await people in the future and how legal rights such as personal rights and privacy can be used.

The number of Deepfake videos is increasing day by day, and the number of false news that emerge increases accordingly. Quality results appear to be too high to realize which news is true or false. People are in a state of chaos and anxiety until they hear or see the true source owners of proof of the accuracy of such videos. In addition, with the emergence of new deepfake software, some of these software, which seems to be a danger to some, have fallen down to smart phones. The software does everything automatically according to a certain order. It is up to the user only to find the necessary pictures.

With the American elections approaching, the banning of deepfake on some social media sharing sites, which is a fear factor, reveals this situation. It is understood from the videos that Deepfake can be used as a visual propaganda tool in the future. A general question comes to mind after Deepfake videos. Can we now trust a video that we don't trust in its source? To conclude from this question, all characters associated with the video will have a headache. Everybody about the video created with Deepfake will try to clear itself or fight legally. Will there be a system to prevent these videos from loading? To date, numerous deepfake videos are displayed on video social networking sites. Considering that many of them have not been given permission from the character owner, how long this video pollution will continue.

Software owners will continue to release advanced versions of deepfake software. The software is usually shaped according to the demands. The next software will automatically create an algorithm that gives you access to your instagram, facebook or personal photos, and will automatically save your photo library that you are investigating to make your deepfake video in a very short time. Therefore, you will need to update your settings on owned social networking sites.

Deepfake videos made from pictures or videos that people share on the internet will have the opportunity to upload to the internet as inappropriate content. Worse still, they can request money from the attacked person simply because of the videos that are allowed to be shared.

Kaynakça / References

Chesney, R. ve , K., D., Citron, (2018). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, Boston University School of Law Scholarly Commons at Boston University School of Law.

Dodge A., House L. ve Johnstone E., Ridder, Costa ve Johnstone, (2019). Using Fake Video Technology To Perpetuate Intimate Partner Abuse Domestic Violence Advisory

Farid .H., Hwang T., Lyu S., Zucconi A., (2019). Deepfakes and Audio-visual Disinformation, Centre for Data Ethics and Innovation (CDEI)

Geradts, Z., Koopman M., Rodriguez M., (2018) Detection of Deepfake Video Manipulation University of Amsterdam & Netherlands Forensic Institute.

Gardiner, N. , (2019) Facial re-enactment, speech synthesis and the rise of the Deepfake, Edith Cowan University.

IEEE SPECTRUM, (2019) "World's First Deepfake Audit Counts Videos and Tools on the Open Web" Erişim Adresi: *https://spectrum.ieee.org/tech-talk/computing/software/the-worlds-first-audit-of-deepfake-videos-and-tools-on-the-open-web*

Koopman Marissa, Macarulla Rodrigez Andrea, Geradts Zeno (2018). "Detection of Deepfake Video Manipulation" University of Amsterdam & Netherlands Forensic Institute

Nguyen T. T. , Nguyen C. M. , Nguyen D. T. , Nguyen D. T., Nahavandi S. (2019) "Deep Learning for Deepfakes Creation and Detection" School of Information Technology, Deakin University, Victoria, Australia

NTV, (2019). 'Deepfake' videoları demokrasileri tehdit ediyor. NTV Web Sitesi. 10 Aralık 2019 tarihinde, https://www.ntv.com.tr/teknoloji/deepfake-videolari-demokrasileri-tehdit-ediyor,7Y_WMt5iZkicDkFRKSlO8A adresinden erişildi.

Paris B., Donovan J. Deepfakes And Cheap Fakes, (2019) "The Manipulation Of Audio And Visual Evidence" Data&Society.

Siekierski, B.J. (2019). Deep Fakes: What Can Be Done About Synthetic Audio And Video?, Economics, Resources and International Affairs Division Parliamentary Information and Resarch Service.

Kaynakça Bilgisi / Citation Information

Berk, M. E. (2020). Dijital çağın yeni tehlikesi "deepfake". *OPUS–Uluslararası Toplum Araştırmaları Dergisi,* 16(28), 1508-1523. DOI: 10.26466/opus.683819