Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

DEEPFAKE'İN ELEKTRONİK ORTAMDA YAPAY ZEKÂ TABANLI KİMLİK DOĞRULAMA SÜRECİNE ETKİSİ

Aybüke GÜNEŞ[1]

Gönderilme Tarihi: 3 Mart 2025
Kabul Tarihi: 20 Mayıs 2025

Review Article / İnceleme Makalesi

Özet

Teknolojik gelişmeler, kimlik doğrulama ile yapılan pek çok işlemin elektronik ortama taşınmasını sağlamıştır. Elektronik ortamda gerçekleştirilen işlemlerin güvenliğinin sağlanması, kimlik doğrulama süreçlerini güvence altına almak için önemli bir ihtiyaç haline gelmiştir. Elektronik ortamda kimlik doğrulama işlemlerinin yapay zekâ kullanılarak gerçekleştirilmesi yapay zekâ tabanlı kimlik doğrulama süreçlerini ortaya çıkarmıştır. Yapay zekâ tabanlı kimlik doğrulama, yüz tanıma ve canlılık teknikleri kullanılarak bireylerin elektronik ortamda kimliklerinin doğrulanmasına imkân tanımaktadır. Ancak, bireylerin fotoğraf ve benzeri görüntülerinden yararlanılarak sentetik video veya görüntüler oluşturulmasına yarayan DeepFake, yapay zekâ tabanlı kimlik doğrulama süreçlerini yanıltmak amacıyla kullanılmaktadır. Bu durum, yapay zekâ tabanlı kimlik doğrulama süreçlerini olumsuz etkilemektedir. Dolayısıyla yapay zekâ tabanlı kimlik doğrulamadaki yüz tanıma sistemlerinin savunma yeteneklerinin, DeepFake saldırılarına karşı artırılması ve güçlü anti-DeepFake tekniklerinin geliştirilmesi gerekmektedir. Bu çalışmada, yapay zekâ tabanlı kimlik doğrulama süreci ve DeepFake incelenmiştir. Bütünsel bir perspektif ile incelemeler yapılması amaçlanmış ve yapay zekâ tabanlı kimlik doğrulama sürecinde DeepFake'in etkisi ele alınmıştır. Sonuç olarak, DeepFake'in olumsuz etkilerinden korunmak için güçlü savunma sistemleri geliştirilmesi, ulusal ve uluslararası alanda birlikte çalışabilirliği artırıcı standart, sertifikasyon ve test yöntemlerinin geliştirilmesi gerektiğine değinilmiştir.

Anahtar Kelimeler: *Kimlik Doğrulama, Elektronik Ortamda Kimlik Doğrulama, Yapay Zekâ Tabanlı Kimlik Doğrulama, DeepFake.*

[1] Bilgi Teknolojileri ve İletişim Kurumu, aybuke.gunes95@gmail.com, ORCID:0000-0003-1027-4905

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

IMPACT OF DEEPFAKE ON ARTIFICIAL INTELLIGENCE BASED IDENTITY PROOFING PROCESS IN ELECTRONIC ENVIRONMENT

Abstract

Technological developments have enabled many transactions carried out with identity proofing to be transferred to the electronic environment. In order to secure identity proofing processes, it has become an important need to ensure the security of transactions carried out electronically. The realization of identity proofing processes in the electronic environment using artificial intelligence has led to the emergence of artificial intelligence-based identity proofing processes. Artificial intelligence-based identity proofing allows individuals to be identity proofing electronically using face recognition and liveness techniques. But, DeepFake, which utilizes photographs and similar images of individuals to create synthetic videos or images, is used to deception artificial intelligence-based identity proofing processes. This has a negative impact on artificial intelligence-based identity proofing processes. Accordingly, it is essential to enhance the defensive capabilities of facial recognition systems in artificial intelligence-based identity proofing against DeepFake attacks and to develop robust anti-DeepFake techniques to mitigate such threats. In this study, the artificial intelligence-based identity proofing process and DeepFake are analyzed. With this study, it is aimed to examine with a holistic perspective and the impact of DeepFake in the artificial intelligence-based identity proofing process is discussed. As a result, it has been mentioned that in order to mitigate the adverse impacts of DeepFake technologies, it is essential to develop robust defense systems, as well as to establish standards, certification frameworks, and testing methodologies that enhance interoperability at both national and international levels.

Keywords: *Identity Proofing, Electronic Identity Proofing, Artificial Intelligence-Based Identity Proofing, DeepFake*

GİRİŞ

Dünyadaki dijital dönüşüm ve teknolojik gelişmeler, fiziksel kimlik doğrulama ile yapılan pek çok işleme ilişkin sürecin elektronik ortama taşınmasını sağlamıştır. Elektronik ortamda hizmetlere erişim sağlamak veya herhangi bir işlemi gerçekleştirebilmek için kimlik doğrulama sürecinin de elektronik ortamda yapılması gerekmektedir. Kimlik doğrulama, bireyin gerçekte iddia ettiği kişi olduğundan belirli bir kesinlik seviyesinde emin olunduğunun belirlenmesi süreciyken elektronik ortamda kimlik doğrulama bahse konu kimlik doğrulama sürecinin elektronik bir yöntemle dijital olarak gerçekleştirilmesi sürecidir. Gündelik yaşamdaki işlemlerin dijital ortama taşınması, bir bireyin kimlik doğrulama işleminin gerçekleştirildiği yerde fiziksel olarak bulunma mecburiyetini ortadan kaldırarak kimlik doğrulama sürecinin elektronik ortamda gerçekleştirilmesini mümkün hale getirmiştir.

Günümüzde teknolojinin gelişmesi ile hayatımızın her alanına etki eden yapay zekâ, elektronik ortamda kimlik doğrulama sürecinin otomatik olarak yürütülmesinde de kullanılmaktadır. Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama, parmak izi ve yüz gibi biyometrik veriler ile kimlik doğrulamaya dayalı olarak gerçekleştirilebilmektedir. Halihazırda sıklıkla tercih edilen yöntem yüz biyometrik verisi kullanılarak yüz karşılaştırması ile kimlik doğrulama yöntemidir. Elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulama süreci, teknolojik gelişmelerin beraberinde getirdiği güvenlik açıkları nedeniyle kötü niyetli bir saldırgan tarafından manipüle edilebilmektedir. Özellikle DeepFake, yüz biyometrik verisine dayanan yapay zekâ tabanlı kimlik doğrulama sistemlerine karşı kötü niyetli saldırganlar tarafından kullanılmaktadır. Kötü niyetli bir saldırgan kimlik doğrulama sürecinin tüm adımlarını biliyorsa ve sahte videoyu kimlik doğrulama sürecine enjekte edebiliyorsa veya videoyu bir ekrana sunabiliyorsa otomatik bir kimlik doğrulama sistemini yanıltması mümkün olabilmektedir. Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinin doğru bir şekilde sonuçlandırılabilmesi ve saldırganların manipülasyonlarından korunabilmesi için güvenlik açıklarına karşı önlemler alınması gerekmektedir.

Bu çalışmada, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecine ve DeepFake'e ilişkin hususlar ele alınmıştır ve bütünsel bir perspektif ile yapay zekâ tabanlı kimlik doğrulama sürecinde DeepFake'in etkisi incelenmiştir. Çalışmanın ilk bölümünde başvuru sahibinin biyometrik verileri kullanılarak

elektronik ortamda gerçekleştirilen yapay zekâ tabanlı kimlik doğrulama süreci ile ilgili bilgilere yer verilmiştir. İkinci bölümde, bireylerin fotoğraf ve benzeri görüntülerinden yararlanılarak sentetik video veya görüntülerin oluşturulmasına yarayan DeepFake teknolojisine dair bilgiler yer almaktadır. Üçüncü bölümde ise, DeepFake'in yapay zekâ tabanlı kimlik doğrulama sürecine etkisi ele alınmıştır. Son olarak çalışmanın sonuçları tartışılarak değerlendirmelere yer verilmiştir.

ELEKTRONİK ORTAMDA YAPAY ZEKÂ TABANLI KİMLİK DOĞRULAMA

Kimlik doğrulama, bireyin gerçekte iddia ettiği kişi olduğundan belirli bir kesinlik seviyesinde emin olmayı ifade etmektedir (NIST, 2017a). Kimlik doğrulama süreci (Şekil 1) genel olarak bireyin tanımlayıcı bilgilerinin toplanması, bireyin tanımlayıcı bilgilerinin gerçek ve doğru olduğundan ve bireyin kimliğinin var olduğundan emin olunması ve kimliğin bireye ait olduğunun teyidinin gerçekleştirilmesi adımlarından oluşmaktadır (AUTHENTICID, 2024).

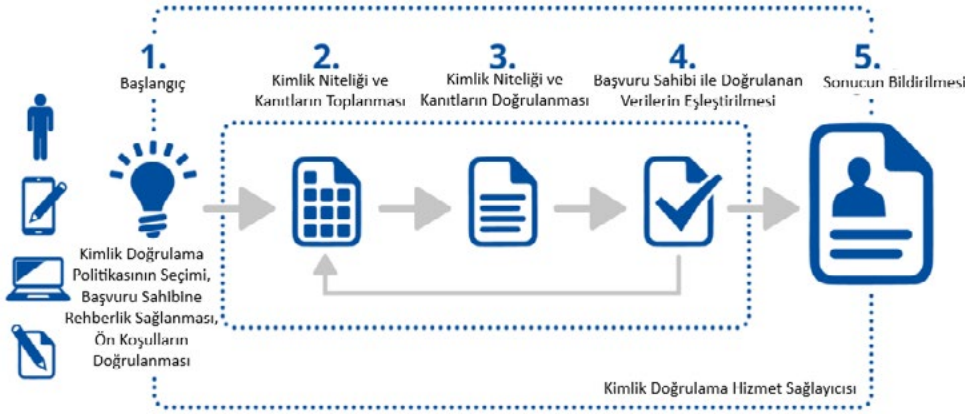
Şekil 1 Kimlik doğrulama süreci (AUTHENTICID, 2024)

Bir bireyin fiziki olarak kimlik doğrulama işlemini yapacak personel ile aynı ortamda bulunmasını gerektiren yani fiziksel mevcudiyete dayalı kimlik doğru-

lama, dünya genelinde yaşanan dijitalleşmenin etkisi ile birlikte elektronik ortamda gerçekleştirilmeye başlanmıştır. Kimlik doğrulama sürecinin elektronik bir yöntemle dijital olarak gerçekleştirilmesi elektronik ortamda kimlik doğrulama sürecini ifade etmektedir.

Elektronik ortamda kimlik doğrulama süreci (Şekil 2), sürecin başlatılması, başvuru sahibinin kimlik niteliği ve kanıtlarının toplanması, toplanan nitelik ve kanıtların doğrulanması, başvuru sahibi ile doğrulanan verilerin eşleştirilmesi ve kimlik doğrulama sonucunun bildirilmesi olmak üzere beş adımdan oluşmaktadır (ENISA, 2021).

Şekil 2 Kimlik doğrulama süreci (ENISA, 2021)



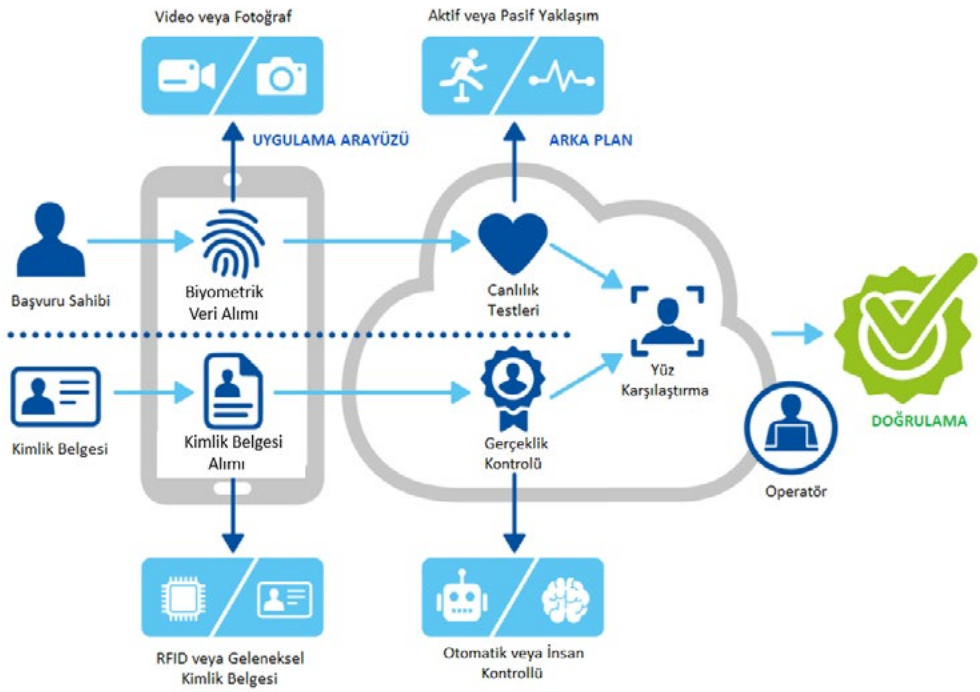
Dijitalleşme ile birlikte, elektronik ortamda kimlik doğrulama sürecinin önünün açılması elektronik işlemlerin çeşitliliğine yönelik potansiyeli artırmış ve işlemlerdeki ilgili tarafların kimliklerinin geçerliliğinin doğrulanabilmesi için kart tabanlı, sertifika tabanlı, mobil tabanlı, biyometrik tabanlı ve çok faktörlü kimlik doğrulama gibi çeşitli yöntemler geliştirilmeye başlanmıştır. Ayrıca elektronik ortamda kimlik doğrulama süreci, günümüz teknolojisinin ilerlemesiyle birlikte açık anahtar altyapısı, blok zincir teknolojisi, yakın alan iletişimi ve yapay zekâ gibi farklı teknolojiler kullanılarak gerçekleştirilebilmektedir (ENISA, 2020).

Esasen, elektronik ortamda kimlik doğrulamanın yapay zekâ ile gerçekleştirildiği bir yaklaşım, yapay zekâ tabanlı kimlik doğrulamayı oluşturmaktadır. Yapay zekâ, kimlik doğrulama süreçlerinin otomatik olarak gerçekleştirilmesini mümkün kılmaktadır. Yapay zekâ tabanlı kimlik doğrulama çözümleri ile bir bireyin

kimliği; yüz, ses ve parmak izi gibi biyometrik veriler ile doğrulanabilmektedir. Ayrıca, kimlik doğrulama süreçlerinde gerçekleştirilen canlılık ve gerçeklik testleri için yapay zekâ algoritmaları kullanılmaktadır.

Elektronik ortamda kimlik doğrulama süreci yapay zekâ ile biyometrik veriye dayalı güvenlik protokolleri oluşturularak gerçekleştirilebilmektedir. Bir bireyin yüz biyometrisi alınarak kimlik belgesindeki fotoğraf ile karşılaştırma yapmak suretiyle yapay zekâ ile kimlik doğrulama gerçekleştirmek mümkündür. Bunun yanı sıra yapay zekâ ile görüntülü kimlik doğrulama sırasında kimliği doğrulanacak birey için canlılık ve gerçeklik testleri de uygulanabilmektedir. Yapay zekâ teknikleri ile herhangi bir insan desteği olmadan otomatik kimlik doğrulama sistemleri oluşturulabileceği gibi operatörlü kimlik doğrulama süreçlerine destek olarak da yapay zekâ teknikleri ile kimlik doğrulama sistemleri kullanılabilmektedir.

Şekil 3 Yapay zekâ tabanlı bir kimlik doğrulama süreci (ENISA, 2022)



Yapay zekâ tabanlı bir kimlik doğrulama sürecine (Şekil 3) göre; ilk olarak başvuru sahibinin kart tabanlı veya geleneksel olan kimlik belgesi ve video kaydı veya fotoğraf kullanılarak biyometrik verisi alınır. Ardından, başvuru sahibinin kimlik belgesinden elde edilen verilerin doğruluğu ve gerçekliği otomatik kontrol veya insan kontrolü ile teyit edilir. Eşzamanlı gerçekleştirilen bu süreç başvuru sahibinin canlılığını gerektirdiği için aktif veya pasif yaklaşımlar kullanılarak canlılık testleri uygulanır. Son olarak başvuru sahibinin biyometrik verisi ile kimlik belgesindeki veriler yapay zekâ ile karşılaştırılır ve sürecin sonunda kimlik doğrulama işleminin kararı ya otomatik bir sistem ile ya da insan denetimi ile sonuçlandırılarak kimlik doğrulama sürecinin çıktısı üretilir (ENISA, 2022).

Elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulamanın süreç adımları; biyometrik verilerin alınması, biyometrik canlılık kontrolü, kimlik belgesi alımı, kimlik belgesi doğruluk kontrolü ve yüz karşılaştırması olmak üzere beş başlık altında gruplandırılabilir.

Biyometrik Verilerin Alınması

Kimlik doğrulamada biyometri kullanımı, hem fiziksel özelliklerin (örneğin parmak izi, iris, yüz özellikleri) hem de davranış özelliklerinin (örneğin, tuş vuruşu hızı) ölçümünü içermektedir (NIST, 2017b). Kimlik belgesi içerisinde bulunan parmak izi veya fotoğraf gibi biyometrik verilerin, yapay zekâ tabanlı bir kimlik doğrulama sürecinde kullanılması, güvenilir kimlik özelliklerinin verimli bir şekilde edinilebilmesi için hem ilgi çekici hem de teknik olarak uygun bir yöntemdir (ENISA, 2021).

Yapay zekâ tabanlı kimlik doğrulama süreci; her zaman bir başvuru sahibinin, kimlik doğrulama sağlayıcısının kendisinden veya güvenilir üçüncü bir taraftan elektronik hizmetlere erişmek ve bu hizmetleri kullanmak için bir kimlik doğrulama hizmetine kaydolmasıyla başlar. Başvuru sahibi ile hizmet sağlayıcı arasındaki güvenli etkileşimin sağlanması için hizmet sağlayıcı tarafından başvuru sahibine iletilen bir mobil uygulama veya bir web tarayıcısı kullanılır. Başvuru sahibi ile hizmet sağlayıcı arasındaki etkileşimin kimliği doğrulanmış güvenli ve korumalı bir kanal üzerinden sağlanması sonrasında, başvuru sahibinin aşağıdakilere ilişkin kanıt sunması gerekir (ENISA, 2022):

- Genellikle başvuru sahibinin video görüntüsü veya bir ya da daha fazla fotoğrafın alınması yoluyla elde edilen yüz özellikleri,

- Elektronik bir belgenin (elektronik kimlik belgesi) çipinde saklanan fotoğraf kullanılarak veya çip ya da şifrelenmiş güvenli ortam olmadığında belge üzerindeki basılı fotoğraf kullanılarak yüz referansının oluşturulabileceği yetkili makamlar tarafından verilmiş geçerli bir kimlik belgesi.

Biyometrik Canlılık Kontrolü

Biyometrik canlılık kontrolü, kameranın önünde yer alan öznenin gerçek ve canlı bir insan olduğuna dair makul güvence elde etmek için başvuru sahibi üzerinde gerçekleştirilen tüm kontrolleri kapsamaktadır. Biyometrik canlılık kontrolü, bir bireyin benzersiz biyometrisini DeepFake kukla, maske veya önceden kaydedilmiş bir video veya fotoğrafın yeniden oynatılması gibi saldırı yöntemleri ile taklit eden bir kopyanın, kimlik doğrulama adımlarını atlatmak için biyometrik tarayıcıya sunulduğu biyometrik sahtekârlık saldırılarına karşı koymak için bir dizi teknik özellik içermektedir (Thales, 2020).

Canlılık kontrolü, güvenli bir uygulamanın en temel unsurları arasında yer almaktadır. Teknik olarak, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama için aktif ve pasif olmak üzere iki tür canlılık kontrolü tespit yöntemi bulunmaktadır (Freiberg, 2024). Bu yöntemler şunlardır:

- **Aktif canlılık tespiti:** Bireylerin süreç sırasında bazı işlemleri yapmasını gerektirmektedir. Aktif canlılık tespitinde, hareketle tetiklenen görüntülerin yakalanması için birey yüzünü kamerayla hizalamalıdır. Ardından bireyin başını sallama, göz kırpma, gülümseme, rastgele sözcükleri okuma, ekranda hareket eden bir nesneyi takip etme, yüzünü kameraya yaklaştırma veya uzaklaştırma, komut üzerine başını sola veya sağa çevirme veya yüzünün önünde elini sallama gibi zorluklara yanıt olarak belirli eylemleri gerçekleştirmesi gerekmektedir (ENISA, 2022).
- **Pasif canlılık tespiti:** Bireylerin süreç sırasında ekstra özel işlemler yapmasını gerektirmemektedir. Pasif canlılık tespitinde, yalnızca bir anlık görüntü alınmakta ve yapay zekâ kullanılarak analiz yapılmaktadır (Freiberg, 2024). Birey yüzünü kamerayla hizalamalıdır. Pasif canlılık tespiti, DeepFake manipülasyonundan kaynaklanan çözünürlük tutarsızlıkları, başvuranın yüzündeki ve çevresindeki yansımaları analiz etmek için birey üzerinde yanıp sönen ışıklar, analiz edilen video çerçevelerinde veya görüntülerde bulunan nabız atışları ve diğer istemsiz insan sinyallerinden kaynaklanan cilt rengi yoğunluğundaki

mikro varyasyonları analiz etme gibi bireyin eylemini gerektirmeyen doğrulama tekniklerine dayanmaktadır (ENISA, 2022).

Aktif canlılık tespiti yaklaşımında, dolandırıcıların fotoğraf saldırıları, video yeniden oynatma saldırıları ve DeepFake gibi tekniklerle elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulama sürecinin kontrollerini atlatması daha zorken; pasif canlılık tespiti yaklaşımında enjekte fotoğraf saldırıları, video yeniden oynatma saldırıları ve DeepFake gibi saldırı tekniklerinin elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulama sürecini atlatması aktif canlılık tespiti yaklaşımındakinden daha kolaydır (Wang vd., 2022).

Kimlik Belgesi Alımı

Kimlik doğrulama için kimlik verilerinin elde edilebilmesi amacıyla başvuru sahibi tarafından ibraz edilen belgenin türüne göre okuma işlemi gerçekleştirilmelidir. Başvuru sahibinin kayıt aşamasında sunduğu kimlik belgesinin türü, bu belgelerin gerçekliğine ilişkin makul güvence elde etmek için gereken kontrol sistemleri üzerinde büyük etkiye sahiptir. Yalnızca kimlik belgesinin ve başvuru sahibinin fotoğrafının yüklenmesinden oluşan bir kimlik doğrulama süreci, kimlik belgesinin ve/veya fotoğrafın manipülasyonuna karşı güvenlik açısından çok zayıf kalacaktır (ETSI, 2021b).

Yalnızca elektronik kimlik belgelerine dayanan elektronik ortamda yapay zekâ tabanlı kimlik doğrulama yöntemi ise erişim ve erişilebilirlik açısından çok sınırlı olacaktır. Bu sınırlamanın başlıca nedenleri; dünya çapında, elektronik kimlik belgelerinin yaygınlığın, geleneksel kimlik belgelerine kıyasla hala ciddi oranlarda az olması ve yakın alan iletişimi okuyucuların, eski ve düşük modelli akıllı telefonlarda yaygın olarak bulunmamasıdır. Diğer yandan geleneksel kâğıt tabanlı kimlik belgelerinin çoğu fiziksel mevcudiyet ile eşdeğer güvence sağlayan araçlar ile gerçekleştirilen elektronik ortamda kimlik doğrulama süreçleri düşünülerek tasarlanmadığından, çok sayıda zorluğa neden olsalar bile hizmetleri geniş çapta erişilebilir kılmaktadırlar (ENISA, 2022).

Elektronik kimlik belgesi veya pasaportun kimlik doğrulama aracı olarak kullanıldığı süreçler bazı güvenlik problemlerini beraberinde getirmektedir. Bu problemlerden biri; başka bir kimlik belgesinin çipinden kopyalanan bir bilgi paketinin kimlik doğrulamasında kullanılan kimlik belgesinin üzerine eklenmesi ile oluşan güvenlik problemidir. Olası diğer bir güvenlik problemi ise; kimlik

doğrulama işlemi esnasında, karşılaştırılmak üzere kimliği doğrulanacak bireyden anlık olarak elde edilen fotoğraf görüntüsü yerine bir saldırı ile farklı bir fotoğrafın kimlik doğrulama sürecinde kullanılması durumudur. Sunucu tabanlı bilgi işlemenin yapıldığı süreçlerde güvenlik önemli bir husustur. Bu sebeple, kimlik doğrulama süreçleri tasarlanırken olası tüm saldırı çeşitleri değerlendirilerek sistem tasarımı yapılmalıdır (ETSI, 2021b).

Kimlik Belgesi Doğruluk Kontrolü

Elektronik ortamda gerçekleştirilecek olan herhangi bir kimlik doğrulama işlemi için öncelikle başvuru sahibinin sunduğu işleme tabi olacak kimlik belgesinin geçerli bir belge olduğu ve sahte olmadığı doğrulanmalıdır. Bir kimlik belgesinin doğrulanması işlemi için, belgenin iptal edilmediğinin ve düzenleyen kurum tarafından geçersiz ilan edilmediğinin kontrolü sağlanmalıdır.

Kimlik belgesi doğruluk kontrolleri, başvuru sahibi tarafından sunulan kimlik belgesinin türüne göre değişiklik göstermektedir. Kimlik belgesinin elektronik olması halinde, kimlik belgesinin çipinde saklanan başvuru sahibinin fotoğrafı gibi kişisel verilerinin kimliğini doğrulamak için açık anahtar altyapısı kullanılmaktadır. Açık anahtar altyapısı, çipte elektronik olarak depolanan verilerin kimliğini doğrulamayı sağlamaktadır. Açık anahtar altyapısında, tüm güvenlik mekanizmalarının tam ve doğru bir şekilde uygulanması, mevcut teknolojilerle yapının ihlâl edilmesini imkânsız hale getirmektedir. Ancak açık anahtar altyapısı mekanizmaları, kimliği doğrulanacak bireyin o anda kimliğini doğrulamak için kullanılan cihazı tuttuğuna dair bir kanıt sağlamamaktadır.

Yalnızca karttan oluşan geleneksel kimlik belgeleri söz konusu olduğunda ise başvuru sahibinin kullandığı cihazın kamerası ile elde edilen deliller üzerinde, optik karakter okuma teknolojisi aracılığıyla veri doğrulama kontrolleri, tutarsızlık ve sahtecilik göstergeleri veya bir yüz fotoğrafının değiştirilmesini tespit etmeyi amaçlayan görsel ve piksel düzeyinde analizler dahil olmak üzere orijinallik kontrolü yapılabilmektedir (ENISA, 2022).

Yüz Karşılaştırma

Elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulamanın yüz karşılaştırma aşamasına geçebilmesi için biyometrik verilerin alınması sonrası gerçekleştirilen canlılık kontrolü adımı ile kimlik belgesi alımı sonrası gerçekleştirilen

kimlik belgesi doğrulama adımlarının başarılı şekilde tamamlanmış olması gerekmektedir.

Yüz karşılaştırma aşamasında gerçekleştirilen yüz tanıma işlemi, genellikle makine öğrenmesi ve derin öğrenme gibi yapay zekâ teknolojilerine dayanmaktadır. Bir bireyin kimliği, biyometrik yüz görüntüsünün fotoğraf veya video ile alınması sonrası yüz tanıma algoritmaları kullanılarak doğrulanmaktadır (Yaman, 2018). Yüz karşılaştırma işlemi, bireyin yüzünün algılanması, algılanan yüz görüntüsünün analiz edilmesi ve yüz eşleştirme oranları değerlendirilerek yüz tanıma işleminin tamamlanması adımlarından oluşmaktadır (Aws, 2023).

Kimliği doğrulanacak başvuru sahibinin yüz görüntüsünün yakalanması için 2D veya 3D sensörler kullanılabilmektedir. Başvuru sahibinin yakalanan yüz görüntüsü belirli algoritmalar ile elektronik bir şablona dönüştürülmekte ve veri tabanında tutulan mevcut şablonlar ile yüz karşılaştırması yapılarak yüz tanıma işlemi sonuçlandırılmaktadır (ENISA, 2020). Yüz tanıma işleminde, zaman içerisinde çok fazla değişiklik göstermeyen gözler arasındaki mesafe, burun genişliği, göz çukurlarının derinliği, elmacık kemiklerinin şekli ve çene hattı uzunluğu gibi bireye ait yüz verilerine odaklanılmaktadır. Günümüzde yüz biyometrisi verilerine dayalı gerçekleştirilen kimlik doğrulama işlemleri, mevcuttaki tek teknoloji ve tek mekanizma olarak kabul edilmektedir (ETSI, 2021b).

Yapay zekâ tabanlı bir kimlik doğrulama sürecinde yüz karşılaştırmasının performansını ölçmek için Yanlış Kabul Oranı (FAR) ve Yanlış Red Oranı (FRR) kullanılmaktadır. FAR ve FRR; parmak izi, yüz ve retina tanıma gibi biyometrik sistemlerin performansını ölçmek için kullanılan güvenlik ölçüleridir. FAR, yanlış bir şekilde geçerli olarak kabul edilen geçersiz girdileri yani yetkisiz bir kullanıcının yanlışlıkla yetkili bir kullanıcı olarak kabul edilme olasılığını temsil etmektedir. Diğer bir ifade ile FAR, biyometrik bir sistemin bir sahtekârdan alınan bir örneği sistemde kayıtlı bir kullanıcının şablonuyla yanlış eşleştirme oranını ölçmektedir. FRR ise, yanlış bir şekilde geçersiz olarak reddedilen geçerli girdileri, yani yetkili bir kullanıcının yanlışlıkla sahtekâr olarak reddedilme olasılığını temsil etmektedir. Diğer bir ifade ile, FRR biyometrik bir sistemin, kayıtlı bir kullanıcıdan alınan veriyi kaç kez başarısız olarak hatalı eşleştirdiğini ölçmektedir (OECD.AI, 2024). Bir sistemin performansı değerlendirilirken kullanılan FAR ve FRR ölçütlerinin dengeli olması gerekmektedir. Kimlik doğrulama için kullanılan sistemdeki özel gereksinimlere ve güvenlik düzeyine bağlı kalarak FAR ve FRR belirlenmelidir.

Günümüzde yaşanan teknolojik gelişmeler ile birlikte ortaya çıkan dijitalleşme, beraberinde kullanılan sistemlerin güvenliğinin sağlanması ve olası tehditlere karşı önlem alınması gerekliliğini getirmiştir. Yapay zekâ tabanlı bir uygulamanın güvenliği, özellikle hassas alanlarda kullanılan yapay zekâ sistemlerinin ve altyapılarının güvenliği için ön koşul kabul edilebilmektedir. Bu nedenle, bir yapay zekâ tabanlı sistemin manipülasyonlara karşı korunabilmesi için doğrulanabilir, izlenebilir ve şeffaf olmasını sağlamak önemlidir. Avrupa Parlamentosu tarafından 2023 yılında kabul edilen ve 1 Ağustos 2024 tarihinde yürürlüğe giren "*Yapay Zekâ Yasası*", güvenlik açıklarına karşı risk barındıran yapay zekâ tabanlı sistemler için şeffaflık yükümlülüğü getirmektedir. Ayrıca yasa, kabul edilemez düzeydeki risklerden minimum risklere kadar dört seviyeli risk temelli bir yaklaşım öngörmektedir. Yasada yer alan bu risk yaklaşımlarından kabul edilemez olanların kullanılmaması, yine yüksek riskli yapay zekâ yaklaşımında, yapay zekâ tabanlı uygulamalar ve hizmetler için potansiyel riskleri en aza indirmek amacıyla devlet kurumları ve özel şirketlerin zorunlu tutulduğu gerekliliklerin olması gerektiği belirtilmektedir (European Parliament, 2023).

Bazı güvenlik riskleri yapay zekâ tabanlı sistemlere özgü olabilmektedir. Örneğin, yapay zekâ tabanlı bir sistemin eğitim verilerinin kirletilmesi ve kullandığı algoritmaların değiştirilmesi ile yapay zekâ tabanlı sistem tehlikeli bir hale getirilebilir. Tanımlanmak istenen bir yüzün doğru şekilde tanımlanmasını önleyebilecek bu tür saldırgan makine öğrenimi tehditleri, yapay zekâ tabanlı sistemlerin güvenliğine yüksek önem verilmesi gerektiğini göstermektedir (ABD National Science and Technology Council, 2016).

Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinin başlangıcından sonuçlanmasına kadarki her aşamasında, güvenlik riskleri ile karşılaşılabilir. Kimlik doğrulama sürecinde kimlik avı saldırıları, kimlik belgeleri üzerinde yapılan sahtecilikler, başvuru sahibine ait biyometrik verilerin manipüle edilmesi gibi güvenlik açıkları olabilir. Yüz karşılaştırması, canlılık kontrolü gibi kimlik doğrulama adımları DeepFake, 3D maske, fotoğraf ve video tekrar saldırıları gibi güvenlik açıkları ile karşı karşıya kalabilir. Dolayısıyla, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama süreçlerinde güvenliğin sağlanması ve güvenlik açıklarının önlenmesi için süreci etkileyecek olası tehditlerin bilinmesi ve tespiti önem arz etmektedir. Bir sonraki bölümde elektronik ortamda yapay zekâ tabanlı kimlik doğrulama süreçlerinde yüz karşılaştırma ve canlılık testi evrelerini olumsuz etkileyen DeepFake saldırısı detaylı bir şekilde incelenmiştir.

DEEPFAKE

Günümüzdeki teknolojik gelişmelere bağlı olarak her geçen gün daha profesyonel hale gelen DeepFake; yapay zekâ, yapay sinir ağları ve yapay zekânın alt dalları olan makine öğrenmesi ile derin öğrenme tekniklerinin kullanılması ile bireylerin fotoğraf ve benzeri görüntülerinden yararlanılarak sentetik video veya görüntülerin oluşturulmasına yarayan bir teknolojidir. Dünya Ekonomik Forumu'na (WEF) göre, DeepFake ile üretilen videoların sayısı her geçen yıl %900 oranında bir artış göstermektedir. DeepFake ile, herhangi bir bireyin yüz ve vücudunun dijital olarak değiştirilmesi ile başka bir birey gibi görünmesine yarayan gerçekçi videolar veya görüntüler elde edilebilmektedir. Elde edilen bu video veya görüntüler, genellikle yanlış bilgilerin yayılması ve diğer kötü niyetli amaçlar için kullanılmaktadır. (CyberMag, 2023).

DeepFake ile oluşturulan sahte videolar, video akışının bazı yazılım veya donanım araçları ile dahili olarak değiştirilmesine neden olan video enjeksiyon saldırıları aracılığıyla elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecini yanıltmak amacıyla kullanılabilmektedir. Video enjeksiyon saldırıları, yazılım ve donanım düzeyi olarak ikiye ayrılmaktadır. Yazılım düzeyinde bir video enjeksiyon saldırısı, kötü amaçlı olmayan bir yazılıma müdahale etmeyi veya kötü amaçlı bir yazılımı gerçek bir uygulama gibi göstermeyi içermektedir. Bir saldırganın, bir cihazın kamerasına yönelik önceden hazırlanmış Deepfake, fotoğraf veya videoları kimlik doğrulama sürecindeki akışa enjekte etmesi yazılım düzeyinde gerçekleştirilen saldırılara örnek olarak verilebilir (Antispoofing, 2024).

Donanım düzeyinde bir video enjeksiyon saldırısı ise bir bilgisayardan gelen HDMI/USB çıkışını, saldırıya uğrayan bir cihaza ait yerel bir video akışıymış gibi maskelemek için kullanılabilmektedir. Burada görüntü veya videonun fiziksel olarak kameraya sunulması yerine donanımsal bir USB bellek veya kameradan video akışını ele geçiren bir JavaScript kodu kullanılarak video enjeksiyon saldırısı gerçekleştirilmektedir (IDR&D, 2024).

Kameraya sunularak veya doğrudan kamera akışına enjekte edilerek gerçekleştirilebilen DeepFake saldırıları özellikle videolu kanıta dayanan kimlik doğrulama süreçlerine karşı kullanılmaktadır. Kötü niyetli saldırgan kimlik doğrulama sürecinin tüm adımlarını biliyorsa ve sahte videoyu kimlik doğrulama sürecine enjekte edebiliyorsa veya videoyu bir ekrana sunabiliyorsa hem otomatik bir

sistemi hem de operatörlü bir kimlik doğrulama sistemini yanıltması mümkün olabilmektedir (ENISA, 2022).

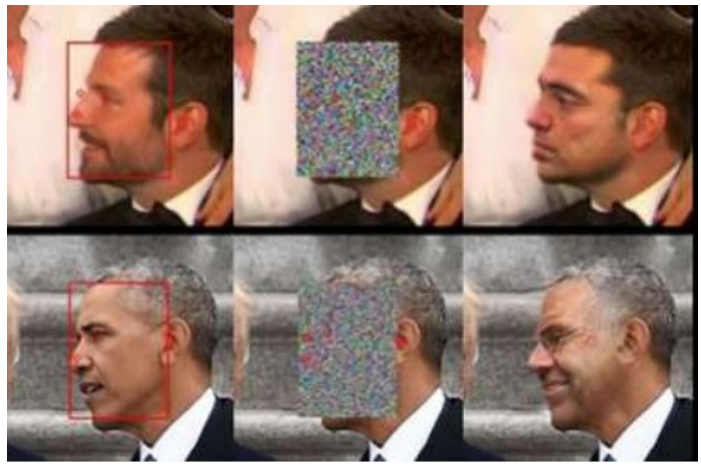
DeepFake'in yüz değiştirme/yerleştirme, ifade değiştirme ve yüz oluşturma olmak üzere bilinen üç yöntemi bulunmaktadır. Bu yöntemler şunlardır (Berk, 2020, s. 1510):

- **Yüz değiştirme/yerleştirme,** hedefteki bir bireyin fotoğrafları kullanılarak bireyin yüzünün başka bir kişiye ait videoya yerleştirilmesi işlemidir (Şekil 4);

Şekil 4 Yüz değiştirme tekniği örneği
((a) orijinal görüntü, (b) DeepFake, (c) hedef birey) (Martı, 2021)

- **İfade değiştirme/yüz yeniden canlandırma/kuklacılık,** kaynak bir videodan elde edilen yüz hareketleri kullanılarak hedefteki bir bireyin yüz videosunun değiştirilmesi işlemidir. Bu yöntem ile hedef kişinin kaş, göz ve ağız ifadelerinin tekrardan oluşturulması ile herhangi bir konu hakkında söylemediği şeyleri söylemiş gibi gösterilmesini sağlayan videolar oluşturulabilmektedir (Şekil 5);

Şekil 5 İfade değiştirme/yüz yeniden canlandırma örneği (Berk, 2020, s. 1510).



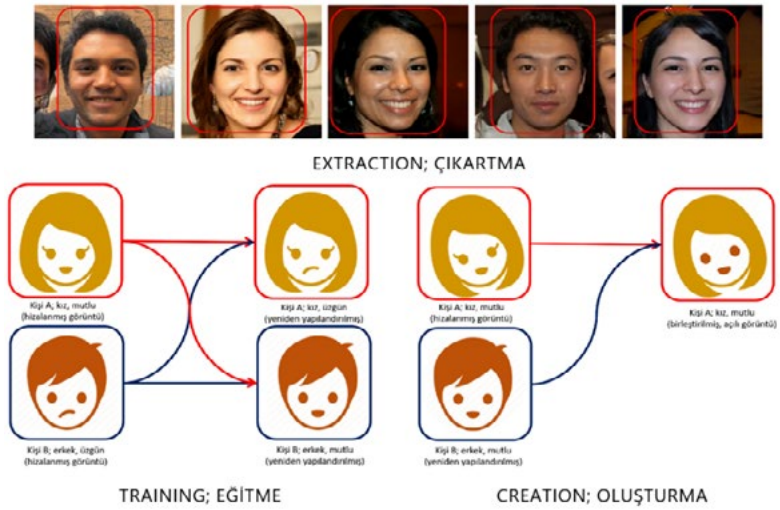
- **Yüz oluşturma,** üretken ve ayrıştırıcı olan iki sinir ağı kullanılarak sahte yüz görüntülerinin oluşturulması işlemidir. Üretken ağın oluşturduğu görüntüler ayrıştırıcı ağ tarafından gerçek olup olmadıkları kontrolünden geçer. Burada amaç üretken kısmın ayrıştırıcı kısmı görüntülerin gerçek olduğuna ikna etmesidir. Ayrıştırıcı kısım üretken kısım tarafından üretilen görüntülerin sahte olduğunu anladığı sürece üretken kısım gerçeğe daha yakın görüntüler üretmeye devam edecektir. Üretken kısım ayrıştırıcı kısmı ikna ederse üretilen görüntü derin öğrenmede kullanılacaktır. Bu yöntem ile pek çok sahte görüntü oluşturulması sağlanmaktadır (Şekil 6).

Şekil 6 Yüz oluşturma örnekleri (Papastratis, 2020).

DeepFake, bir veya daha fazla fotoğraftan başlayarak istenildiği zaman kontrol edilebilen etkileşimli bir 3D dijital kukla kullanılarak da yapılabilmektedir. Bu, saldırganlar tarafından üç boyutlu modeller oluşturmaya yönelik yazılımlar kullanılarak gerçekleştirilebilmektedir. Günümüzde, DeepFake videoları ve etkileşimli DeepFake 3D dijital kuklaları gerçek zamanlı olarak oluşturulabilir durumdadır. Gerçek zamanlı olarak gerçekleştirilen bir saldırı ancak yüksek kalitede ve büyük miktarda bilgi işlem gücünün mevcut olmasıyla elde edilebilmektedir. Dolayısıyla uygulanması oldukça zordur. Ancak, yaşanan teknolojik gelişmelerin etkisi ile bu zorluk engeli her geçen gün azalmaktadır. Günümüzde popüler olan mobil uygulamalardan herhangi biri kullanılarak akıllı telefonlarda oldukça ikna edici DeepFake'ler oluşturulabilmektedir (ENISA, 2022).

Video yapımı ve özel efektler hakkında derin bir bilgiye sahip olmaya gerek kalmadan, makine öğreniminden yararlanan güçlü video işleme ve artırılmış gerçeklik teknikleri ile görüntüsü elde edilebilen herkesin DeepFake videosunun oluşturulması kolay bir hale gelmiştir. Ses klonlama yöntemleri ile daha gerçekçi hale getirilebilen DeepFake'in temel zorluğu, saldırganın, videosunu oluşturmak istediği hedef bireye ait fotoğraf veya videolarından oluşan geniş bir veri kümesine ihtiyaç duymasıdır. Veri kümesinde yer alan hedef bireye ait fotoğraf veya görüntüler yardımı ile DeepFake videosu oluşturmak için kullanılan program eğitilmekte ve eğitim sonucunda öğrenilen bilgiler ile sahte videonun oluşturulması sağlanmaktadır (ENISA, 2022).

Şekil 7 DeepFake temel adımları (Atmaca ve Bakırcı, 2019).



DeepFake'nin çalışma mantığında; veri toplama ve kodlayıcı-kod çözücü adımları ile birlikte çıkartma, eğitme ve oluşturma temel adımları (Şekil 7) olmak üzere genel olarak aşağıda açıklanan beş aşamadan bahsedilebilmektedir (Atmaca ve Bakırcı, 2019; Bernaciak ve Ross, 2022).

- **Kaynak ve hedef videonun toplanması aşaması,** kaynağa ve hedefe ait 4K kalitesinde videoların edinilmesi aşamasıdır. Bu aşamada, DeepFake'in inandırıcı olması ve başarılı sonuçlar verebilmesi için kaynağın ve hedefin benzer yüz şekline ve boyutuna sahip olması, cilt tonu renklerinin benzer olması ve aynı cinsiyete sahip olmaları gibi dikkat edilmesi gereken bazı hususlar mevcuttur.
- **Çıkartma (Extraction) aşaması,** eğitim aşaması öncesi ihtiyaç duyulan büyük miktardaki verinin, hedef bireyin çeşitli yollarla toplanan videolarından ayrıştırılan görüntü parçacıklarından elde edilmesi aşamasıdır.
- **Eğitme (Training) aşaması,** çıkartma aşamasında elde edilen görüntü parçacıkları kullanılarak yapay sinir ağının bir görüntüyü diğer bir görüntüye dönüştürmesi için eğitildiği aşamadır.
- **Dönüşüm aşaması,** bir dizi yüz görüntüsünün kodlayıcı ve kod çözücü ağından tek yönlü olarak geçirildiği ve çıktı olarak bir yazılım aracılığıyla video oluşturabilecek kareler elde edildiği aşamadır.
- **Oluşturma (Creation) aşaması,** DeepFake yazılımının birleştirme özelliğinden yararlanılarak DeepFake'in oluşturulduğu aşamadır. DeepFake yazılımı, derin öğrenme işlemlerinde kullandığı kaynaktan elde edilen fotoğraf veya video verilerinden çıkardığı görüntü parçacıklarını hedefteki yüz görüntüsüne yerleştirmek için programlanmıştır. Kaynaktan elde edilen yüz görüntüleri ne kadar çok ve kaliteli olursa bu aşamanın sonucunda elde edilen video da o derece başarılı olacaktır.

Tüm bunların yanında, DeepFake'in hareketli bir görüntü dışında hareketsiz donuk kareler üzerinde de oluşturulabileceği bilinmektedir. Hatta, DeepFake'in donuk bir kare üzerindeki manipülasyonuna örnek olarak İtalyan ressam Leonardo da Vinci'nin ünlü eseri Mona Lisa'nın yüz ifadesi değiştirilerek oluşturulmuş bir örnek (Şekil 8) bulunmaktadır (Elitaş, 2022, s. 113).

Şekil 8 DeepFake ile gerçekleştirilen donuk kare manipülasyonu (Elitaş, 2022, s. 113).

DeepFake saldırılarının zorluklarından birinin iyi bir veri kümesinin toplanması gerekliliği olmasının yanı sıra unutulmaması gereken bir diğer faktör ise zaman faktörüdür. Pek çok algoritmanın programlandığı görevi gerçekleştirmek için belirli bir hedef üzerinde saatlerce eğitilmesi gerekmektedir. Ancak gelecekteki teknolojik ilerlemeler ile birlikte işlem gücünün gelişmeye devam etmesinin, DeepFake oluşturulurken kullanılan algoritmaların zaman sorununu çözmesi beklenmektedir (ENISA, 2022).

Ayrıca, DeepFake gerçek olanı manipüle etme noktasında yalnızca görüntüler üzerinde veri işlememektedir. DeepFake, gerçekliğin yansıtıcısı olan sesin de derin sinir ağları ile simüle edilmesinde kullanılabilmektedir. Görüntüler üzerinde gerçekleştirilen işlem adımlarına benzer şekilde sesin öğrenilmesi de detaylı bir süreç gerektirmektedir. Bu süreçte sesi taklit edilmek istenen hedef bireye ait ağız hareketleri, tonlama ve vurgulama gibi bireyin sesine ilişkin belirleyici özelliklere dair çok fazla veriye ihtiyaç duyulmaktadır (Elitaş, 2022, s. 113).

Ses manipülasyonu ile kimlik doğrulama sürecinde bir operatör varsa gerçek bir kişiyle etkili bir şekilde konuşuyormuş gibi olacak ve bu kimlik doğrulama sürecinin bir sahtekâr tarafından atlatmasına ihtimal verecektir. 2020 yılında, bir grup hacker "*Business Identity Compromise*" isimli bir yöntem ile Hong Kong bankasından DeepFake ses simülasyonu aracılığıyla 35 milyon dolar çalmayı başarmıştır. Gerçekleştirilen bu soygun dünya genelinde maddi kaybı en yüksek olan olay olarak kabul edilmiştir. Business Identity Compromise, DeepFake teknolojisini kullanan genellikle bir kuruluşun üst düzey yöneticilerinin bilgi ve

sesini kopyalayarak gerçekleştirilen bir saldırı modelidir. Görüntü veya videolara uygulanan DeepFake'ler ile yapılan içerikler ses klonlamalarıyla daha gerçekçi hale gelmektedir. DeepFake'teki ses klonlamaları, monoton konuşma şekli ve metalik ses ile kendini ele verebilmektedir (STM ThinkTech, 2023).

Ek olarak, DeepFake'in görüntüler üzerindeki etkisi elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecini etkileyerek sürecin manipülasyonuna neden olabilmektedir.

YAPAY ZEKÂ TABANLI KİMLİK DOĞRULAMA SÜRECİNDE DEEPFAKE

Yapay zekâ ve makine öğrenimi gibi disiplinlerin rekabet ettiği günümüzde araştırmacılar, kimlik doğrulama süreçlerini mümkün olduğunca otonom hale getirmenin yollarını araştırmaktadır. Ancak, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinde süreci etkileyen DeepFake gibi saldırılar bireylerin kimliğinin doğrulanabilmesi için kullanılan tekniklerin uygulamasının önünde büyük bir sorun teşkil etmektedir.

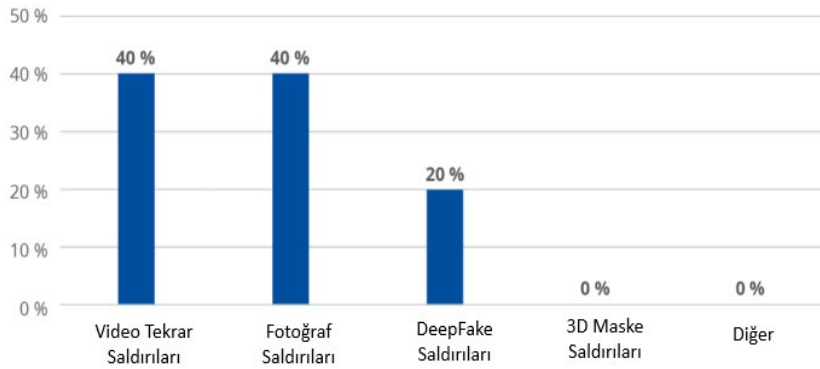
Elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulama sürecinde kullanılan web veya mobil uygulamanın amacı, güvenli bir şekilde başvuru sahibine ait kimlik kanıtlarının toplanmasını sağlamaktır. Ancak dışarıdan gelecek kötü amaçlı herhangi bir müdahale ile kimlik doğrulama sisteminde kullanılan cihazın kamerası manipüle edilebilmektedir. Yani saldırgan kimlik doğrulama sistemine gönderilen video akışını değiştirmek için kimlik doğrulama uygulamasının mimarisine müdahale edebilmekte ve sahte videolar cihaz kamerasından geliyormuş gibi kimlik doğrulama sistemine kanıt olarak sunulabilmektedir.

Günümüzde, film sektörü gibi sektörlerde bir aktörün daha genç veya yaşlı gösterilmesi gibi iyi niyetli amaçlar için DeepFake teknolojisi kullanılsa da DeepFake teknolojisinin iyi niyetli amaçlar dışında kullanılmasının büyük riskler oluşturduğu bilinmektedir. Son yıllarda teknolojide yaşanan gelişmeler son derece gerçekçi görüntüler ve videolar üretmekte kullanılan DeepFake teknolojisinin tespit edilmesini zorlaştırmaktadır. Bazı karmaşık olmayan DeepFake görüntü ve videolarının tespitinde aktif veya pasif kontrollerin etkili olduğu, ancak daha karmaşık bir yapıya sahip DeepFake'lerin gerçeğe yakın görüntü ve video sunmasının elektronik ortamda yapay zekâ tabanlı kimlik doğrulama kontrollerini

atlatmasına olanak tanıdığı düşünülmektedir (STM ThinkTech, 2023).

Son dönemlerde, mevcut saldırıların başarı oranları göz önüne alındığında DeepFake saldırılarının giderek yaygınlaştığı ve geleceğe yönelik en endişe verici saldırılar arasına girdiği (Şekil 9) görülmektedir (ENISA, 2022). Saldırganın hedefin gerçek görüntülerini veya ham videolarını kimlik doğrulama sistemine enjekte ederek kullandığı basit düzeydeki saldırılar aktif ve pasif canlılık kontrollerini atlatmak için yeterli olmamaktadır. Ancak yeni ortaya çıkan ve gelişmiş DeepFake'ler kimlik doğrulama sistemlerindeki aktif ve pasif canlılık kontrollerini atlatabilmektedir.

Şekil 9 Mevcut saldırıların başarı oranları (ENISA, 2022)



Gelecekteki tehditler arasında sayılan ve yasa dışı veya etik olmayan amaçlar için kullanılabilen DeepFake; görüntü, ses ve video oluşturmak veya değiştirmek için orijinal görünen sentetik içerikler sağlayan yapay zekâ tabanlı bir teknolojiyi ifade etmektedir. Teknolojik olarak sürekli gelişim gösteren ve dijital medyayla birbirine bağlanan dünyada DeepFake oluşturma maliyetlerinin önemli ölçüde azalmasıyla birlikte, DeepFake'ler değişik sektörlerde önemli bir hale gelmiştir. DeepFake'ler eğitim, sanat, dijital yeniden yapılanma, kamu güvenliği ve eğlence endüstrisi gibi farklı sektörleri dönüştürme potansiyeline sahip olduğu gibi kötü niyetli saldırganlar tarafından saldırı amaçlı da kullanılabilmektedir (ENISA, 2023a).

Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinin bir mobil uygulama veya web uygulaması üzerinden telefon veya bilgisayara ait kameralar

kullanılarak gerçekleştirilmesi, DeepFake kullanılarak gerçekleştirilen video enjeksiyon saldırılarına karşı sistemi savunmasız kılmaktadır. Cihazın kontrolünün saldırganda olması, her türlü güvenliğin saldırgan tarafından aşılabilmesi, yeni güvenlik açıklarına karşı daha sağlam yöntemlerin geliştirilmesi gerektiğini göstermektedir. Bir cihazı manipüle eden saldırıların önüne geçebilmek için saldırı adımlarının iyi bilinmesi gerekmektedir. Cihaz manipülasyonu ile saldırı gerçekleştirme işleminin adımları şunlardır (Carta vd., 2022, s. 92):

- Saldırı için kullanılacak cihazın kontrollerini sıfırlamak,
- Kimlik doğrulama işleminin gerçekleştirileceği uygulamanın gizliliğini kaldırmak,
- Uygulamanın kodunu kaynak koda dönüştürmek,
- Uygulamanın hangi işlevlerinin kamerayı çağırdığını, kamera tarafından çekilen görüntülerin nerede saklandığını ve görüntü formatını tespit etmek,
- Kamera tarafından alınan bilgileri yeniden yönlendirerek saldırı cihazından gelen görüntüleri kameradan geliyormuş gibi kimlik doğrulama sistemine yönlendirmek.

Saldırgan saldırıları iki farklı şekilde sisteme enjekte edebilmektedir (Carta vd., 2022, s. 92):

- Enjekte edilecek videolar, uygulama tarafından talep edilen talimatlara göre gerçek zamanlı olarak yeniden yapılandırılabilir; veya
- Enjekte edilecek videolar, uygulamanın hafızasında kayıtlı olan talimatlara göre önceden hazırlanabilir.

Gerçek zamanlı video yapılandırılmasında saldırganın daha fazla çalışması gerekir, ancak video akışında herhangi bir kusur görünmez ve son videoyu oluşturmak için zaman kaybı yaşanmaz. Önceden hazırlanan videolar ise saldırgan açısından kolaylık sağlasa da video akışında oluşacak kesintiler (örneğin; kafanın konumunda yaşanacak değişiklikler) saldırı için dezavantaj oluşturmaktadır (Carta vd., 2022, s. 92).

Bununla birlikte, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecindeki yüz tanıma sistemine uygulanan manipülasyonlardaki DeepFake'ler üç şekilde tanımlanabilmektedir (STM ThinkTech, 2023):

- Bir bireyin yüz görüntüsü başka bir bireyin yüz görüntüsü ile değiştirildiğinde yüz görüntüsünün bazı noktalarında ten rengi ve doku geçişlerinden kaynaklı bozulmalar söz konusu olabilir.
- Özelikle bireyin diş ve gözlerinde yer alan detaylarda fark edilebilir derecede dokusal farklılıklar ve bulanık görünmeler olabilir.
- Bireyin yüz ifadelerinde veya aydınlatma sonucu yüzde oluşan gölgelenmelerde başın hızla hareket ettirilmesi sonucu hatalar oluşabilir.

Güvenlik açıklarına karşı, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinde kimlik kanıtı olarak başvuru sahibinden toplanan verilerin güvenliği için hizmet sağlayıcı sistemleri üzerinde önlemlerinin alınması, ek olarak başvuru sahibinin yapay zekâ tabanlı kimlik doğrulama süreci için kullandığı cihaz kamerası ile işletim sistemi arasında karşılıklı kimlik doğrulama ve güvenli iletişim kanalı protokollerinin uygulanması gibi çözümler önerilmektedir. Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama için kullanılan sisteme DeepFake'in enjekte edilmesinin önüne geçilebilmesi için kimlik doğrulamanın gerçekleştirildiği cihazın kurcalamaya karşı korumalı olması da gerekmektedir (Carta vd., 2022, s. 92).

Tipik bir yüz tanıma içeren elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sistemi,

- Sisteme kayıtlı bir yüz kimliğine karşı kimlik doğrulama tanımlayıcısı olarak başvuru sahibi tarafından sağlanan tek bir fotoğrafı kullanan görüntü tabanlı,
- Başvuru sahibinin kendi video klibini yüklemesini gerektiren sessizliğe dayalı,
- Başvuru sahibinin kimlik doğrulama sistemi tarafından belirlenen eylemleri gerçekleştirmesini gerektiren eylem tabanlı,
- Bir başvuru sahibinin istemli konuşmasını, o kullanıcının konuşma modeli için sistemin veri tabanı girişiyle eşleştiren ses tabanlı olmak üzere dört farklı vektörden biri ile oluşturulabilmektedir. Her bir vektörde farklı saldırı türü ile karşılaşılabilmektedir.

Bu saldırı türlerinin önüne geçmek için mevcut teknolojilerde;

- Kimlik doğrulamanın başvuru sahibinin kamera akışındaki tek bir kareye dayandığı görüntü tabanlı kimlik doğrulama yönteminin terk edilmesi,

- Görüntü ve ses alanlarında DeepFake tespit sistemlerinin daha esnek ve kapsamlı bir şekilde güncellenmesi,
- Başvuru sahibinin videosundaki ses tabanlı kimlik doğrulamanın dudak hareketleriyle senkronize edilmesinin zorunlu olması ve
- Başvuru sahibinin DeepFake sistemleri tarafından yeniden üretilmesi henüz mümkün olmayan yüzün kısmi olarak karartılması veya profil görünümlerinin sağlanması gibi jest ve hareketleri gerçekleştirmesinin zorunlu tutulması gibi yöntemler ile iyileştirmelerin yapılmasının olumlu sonuçlar vereceği düşünülmektedir (Wang vd., 2022; Anderson, 2022).

Son dönemlerde araştırmacılar, akademisyenler, özel şirketler ve farklı kurum ve kuruluşlar tarafından elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecini olumsuz etkileyen saldırılar derinlemesine incelenmekte olup bu saldırılara karşı çeşitli önlemler geliştirilmesine yönelik çalışmalar artırılmaktadır.

Bir DeepFake saldırısına karşı alınan her türlü önlem, anti-DeepFake olarak isimlendirilmektedir. Anti-DeepFake için kullanılacak algoritmalar yüksek düzeyde veriye ihtiyaç duymaktadır. Bu veri ihtiyacının karşılanması amacıyla Facebook Meta ve diğer sektör liderleri tarafından 100.000'den fazla video içeren "*Deepfake Detection Challenge Dataset*" isimli bir veri seti oluşturulmuştur. Oluşturulan veri seti ile DeepFake tespit yöntemlerindeki ilerlemelerin ölçülmesi hedeflenmektedir. Dünyanın dört bir yanından uzmanlar bir araya gelerek DeepFake tespit modellerinin kıyaslanmasına, yeni yaklaşımların denenmesine ve birbirlerinin çalışmalarından yeni şeyler öğrenmelerine, oluşturulan veri setini kullanarak olanak sağlamaktadır (Facebook Meta, 2020). Deepfake Detection Challenge Dataset gibi veri setlerinin oluşturulması anti-DeepFake modellerinin geliştirilmesinin önünü açmaktadır.

Videolardaki anormal göz hareketleri, orantısız parlaklıklar, renk ve ışıkta yaşanan uyumsuzluklar DeepFake'in tespit edilmesinde yardımcı unsurlardır. Mevcut DeepFake'ler dili, ağız içini ve dişleri tam olarak detaylandırmadığından bu alanlardaki bozulmalar DeepFake'i ele verebilmektedir. Bununla birlikte, anti-DeepFake için yapay zekâ yazılımları kullanılabilir. Gelişmiş yapay zekâ teknikleri ile geliştirilmiş yazılımlar yine yapay zekâ teknikleri ile oluşturulmuş DeepFake görüntü ve videolarındaki bozulmaları kolaylıkla tespit edebilir. Ancak anti-DeepFake alanında uluslararası standartların ve düzenlemelerin bulunmaması nedeniyle teknik sorunlar yaşanabilmektedir (STM ThinkTech, 2023).

Bununla birlikte, Amerika Birleşik Devletleri ve Çin arasında kurulan yeni bir araştırma birliği tarafından, yüz tanıma içeren dünyadaki en büyük kimlik doğrulama sistemleri üzerinde DeepFake duyarlılık testleri geçekleştirmiş ve gerçekleştirilen testlerin sonucunda, yeni ortaya çıkan ve her geçen gün gelişen DeepFake saldırılarına karşı yüz tanıma sistemlerinin bazılarının, savunmasız olduğu ortaya çıkarılmıştır. Birçok müşteriye hizmet veren kimlik doğrulama sistemlerindeki DeepFake tespit etme modüllerinin çok fazla hata içerdiği ve kimlik doğrulama sistemlerinde eskimiş DeepFake tekniklerinin kullanılmasının hata oranını artırdığı belirtilmiştir. Ek olarak, genel yüz tanıma sistemlerinde yer alan mevcut konfigürasyonların kadın ve beyaz olmayan bireyleri içermeyerek yalnızca beyaz erkeklere yönelik oluşturulmasının DeepFake riskini kadın ve beyaz olmayan bireyler için artırdığı tespit edilmiştir. Bu durum, belirli bir grup insan için önemli güvenlik riskleri oluşturabilecek hususların bulunduğunu göstermektedir (Anderson, 2022).

Ayrıca, Çin DeepFake faaliyetleriyle ilişkili tehlikeleri azaltmak amacıyla derin sentez/DeepFake teknolojisine ilişkin derin sentez hizmet sağlayıcıları ve kullanıcılarını içeren hükümler yayımlamıştır. Hükümler genel olarak, metin oluşturma veya değiştirme, ses içeriği oluşturma veya değiştirme, konuşma dışı içerik oluşturma veya değiştirme, yüz oluşturma veya değiştirme gibi teknikleri kapsamaktadır. Derin Sentez Hükümleri, derin sentez hizmet sağlayıcılarının ana yükümlülüklerini açıkça belirtmektedir. Derin Sentez Hükümlerine göre derin sentez hizmet sağlayıcıları; veri güvenliği ve kişisel verilerin korunması, şeffaflık, içerik yönetimi ve etiketleme, teknik güvenlik gibi yükümlülükleri yerine getirmekle sorumlu tutulmaktadır (Interesse, 2022; Çin Siber Uzay İdaresi, 2022).

Sonuç olarak, elektronik ortamda yapay zekâ tabanlı bir kimlik doğrulama sürecinde güvenliğin sağlanması ve güvenlik açıklarının önlenmesi için süreci etkileyecek DeepFake gibi olası tehditlerin bilinmesi, tespiti ve bu saldırılara karşı anti-DeepFake önlemlerinin her geçen gün geliştirilmesi önem arz etmektedir.

DEĞERLENDİRME

Dijitalleşme ile birlikte, önem kazanan elektronik ortamda yapay zekâ tabanlı kimlik doğrulama yöntemi, kimlik belgesinde yer alan yüz fotoğrafının başvuru sahibinin canlılığı kanıtlanmış yüz görüntüsü ile karşılaştırılmasına dayanmaktadır. Bu kimlik doğrulama yönteminde, sürecin kötü niyetli bir saldırgan tarafından manipüle edilme ihtimali her zaman mevcuttur. Kimlik doğrulama süreçlerinin vazgeçilmez bir parçası olan kimlik belgesine ve bir bireyin benzersiz şekilde tanınmasına olanak veren yüz görüntüsünün kimlik doğrulama sürecinde kullanılmasına ilişkin bazı güvenlik açıkları ile karşılaşılabilmektedir. Kimlik doğrulama sürecinin doğru bir şekilde sonuçlandırılabilmesi ve saldırganların manipülasyonlarından korunabilmesi için güvenlik açıklarına karşı önlemler alınması gerekmektedir.

Dijitalleşme ile gelen güvenlik hususu sistemlerin donanımsal güvenliğinden yazılımsal güvenliğine ve vatandaşların kişisel bilgilerinin korunmasına kadar pek çok konu ile ilişkilendirilebilmektedir. Bir yapay zekâ sistemi, kendi güvenlik açıkları veya bağlı olduğu diğer mekanizmaların güvenlik açıkları nedeniyle güvenlik tehditlerine karşı savunmasız kalabilmektedir. Güvenli bir yapay zekâ sisteminin geliştirilmesi, geliştirme aşamasından son aşamaya kadar her aşamada güvenlik açıklarının ve risklerinin dikkate alınmasını içermektedir (ENISA, 2023b).

Günümüzde DeepFake teknolojisinin anti-DeepFake tekniklerinden daha hızlı bir şekilde gelişiyor olması ve DeepFake saldırıları ile kimlik doğrulama sistemlerinin aldatılabilmesi nedeniyle yüz tanımanın kimlik doğrulama sistemlerinde tek başına kimlik doğrulama çözümü olarak kullanılması tavsiye edilmemektedir. Yapay zekâ yazılımı ile otomatikleştirilmiş kimlik doğrulama sistemlerinde, yapay zekânın başvuru sahibini tanımlamak için kullandığı doğruluk yüzdesinin önceden belirlenmiş bir eşik değerinin üzerinde olması gerekmektedir. Doğruluk değerinin bu eşik değeri altında kaldığı durumlarda kimlik doğrulama işlemi için insan müdahalesi gerekli olabilmektedir. Bu durumda, bir insan operatör aracılığıyla başvuru sahibinin kimliğinin doğrulanma işlemi teyit edilebilir. Yapay zekâ, yüz karşılaştırması gibi görevlerde insanlardan daha yetenekli olabilmesine rağmen, fotoğrafların çekildiği alanları analiz etmesi gibi görevlerde iyi değildir. Bu da fotoğraflarda yer alan bağlamsal öğelerin tespit edilmesi, başvuru sahibinin bilinçsiz olduğu veya tehdit edilerek kimlik doğrulama süreçlerine zorlandığı

gibi durumların tespitinde yine insan müdahalesinin gerekebileceği anlamına gelmektedir. Teknolojik gelişmelere bağlı olarak, yapay zekânın ihtiyaç duyduğu büyük veri sorunlarının hallolması ile bu durumun değişebileceği düşünülmektedir. Ancak şimdilik yapay zekâ tabanlı bir kimlik doğrulama sürecinde insan operatörlere de ihtiyaç duyulmaktadır (ENISA, 2022).

Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama sürecinde karşılaşılabilecek saldırılara karşı hangi önlemin uygulanacağına dair net bir seçim bulunmamaktadır. Yapay zekâ tabanlı kimlik doğrulama yöntemini kullanacak işletmenin türü, işletmenin hizmet verdiği kullanıcının türü ile sayısı ve işletmenin kimlik doğrulama sürecinde elde etmek istediği güven düzeyi gerçekleştirilen kimlik doğrulama sürecini manipüle etmek için kullanılabilecek saldırılara karşı alınacak önlemlerin seçimi ile doğrudan ilişkidir. Mühendislik problemlerinin pek çoğunda olduğu gibi kimlik doğrulama sürecinde alınacak karşı önlemleri seçerken kullanılabilirlik ve etkinlik arasında doğru bir denge oluşturmak gerekmektedir. Ancak kullanılacak karşı önlemlerin etkinliği konusunda %100'lük bir güvenceye ulaşmak mümkün değildir. Karşı önlemlerin temel amacı, sahtekârlığı gerçekleştirmenin zorluğunu ve maliyetini elde edilecek potansiyel faydalardan daha yüksek tutmaktır (ENISA, 2022).

Bununla birlikte dünya genelinde ülkeler ve uluslararası kuruluşlar dijital güvenlikle ilgili araştırmalar yaparak güvenlik açıklarına karşı oluşabilecek tehditlerin, saldırıların ve siber olayların tespiti ve yönetimine yönelik zorlukları ele almaya çalışmaktadır. Ayrıca, ülkeler ve uluslararası kuruluşlar tarafından kimlik doğrulama, yapay zekâ ve DeepFake gibi pek çok konuda çalışmalar yürütülmektedir (Tablo 1).

Tablo 1 Bu çalışmada bahsi geçen ülkeler ve uluslararası kuruluşların çalışmalarına ilişkin özetler

ÜLKE/ KURULUŞ	ÇALIŞMA ADI	İÇERİK
ABD	National Science and Technology Council	Algoritmaların manipüle edilmesi gibi yapay zekâlı sistemlere özgü bazı güvenlik riskleri ele alınmaktadır.
Çin Siber Uzay Ajansı	Provisions on the Administration of Deep Synthesis Internet Information Services	DeepFake faaliyetleriyle ilişkili tehlikeleri azaltmayı amaçlayan hükümler yayımlanmıştır.
ENISA	eIDAS Compliant eID Solutions	eID araçları için kullanılan temel teknolojilerle ilgili güvenlik hususları ve öneriler ele alınmaktadır.
ENISA	ENISA Remote ID Proofing	Kimlik doğrulama için en yaygın yöntemlere genel bir bakış sunulmaktadır.
ENISA	ENISA Remote Identity Proofing- Attacks & Countermeasures	Yüz tanıma sistemlerini kandırmayı amaçlayan yüz sunumu saldırıları ele alınmaktadır.
ENISA	Identifying Emerging Cyber Security Threats and Challenges for 2030	Gelecekteki siber güvenlik tehditleri araştırılmaktadır.
ENISA	Artificial Intelligence and Cybersecurity Research	Siber güvenlik için yapay zekâ ve yapay zekânın güvenliğini sağlama konusunda araştırma ihtiyaçlarını belirlemektedir.

ETSI	ETSI TS 119 461 V1.1.1 (2021-07)	Güven hizmeti konularının kimlik doğrulamasını sağlayan güven hizmeti bileşenleri için politika ve güvenlik gereksinimlerini belirtmektedir.
ETSI	ETSI TR 119 460 V1.1.1 (2021-02)	Güvenilir hizmetlere ilişkin kimlik doğrulama teknolojileri ve düzenleyici gereklilikleri incelenmektedir.
European Parliament	Artificial Intelligence ACT	Yapay zekâ sistemlerine risk temelli bir yaklaşım getirerek belirli sınıflara ayrıştırılması amaçlanmaktadır.
NIST	Digital Identity Guidelines.	Dijital kimlik hizmetlerine ilişkin teknik gereksinimler sağlamaktadır.
NIST	Digital Identity Guidelines Authentication and Lifecycle Management.	Dijital kimlik hizmetlerini kullananlar için kimlik doğrulama ve yaşam döngüsü yönetimi gereksinimlerini sunmaktadır.
OECD.AI	Catalogue of Tools & Metrics for Trustworthy AI.	Yapay zekânın güvenilirliğini ve risklerini ölçmek ve değerlendirmek için teknik metrikler ve metodolojiler içermektedir.

SONUÇ

Elektronik ortamda kimlik doğrulama işlemleri tüm dünyada olduğu gibi ülkemizde de temel bir öneme sahiptir ve dijital dönüşüm hamleleri ile birlikte giderek daha fazla önem kazanmaktadır. Ancak yapay zekâ tabanlı kimlik doğrulama yöntemini tercih eden ülkelerin sayısı ve bu konuya ilişkin düzenlemeler sınırlı olmakla birlikte henüz net bir standart veya düzenleme de bulunmamaktadır. Ayrıca, ülkelerin yapay zekâ tabanlı kimlik doğrulama süreçlerindeki güvenlik hususlarına ilişkin özel düzenlemelerinin de henüz bulunmadığı bilinmektedir.

Kimlik belgesinde yer alan yüz fotoğrafının başvuru sahibinin canlılığı kanıtlanmış yüz görüntüsü ile karşılaştırılmasına dayanan elektronik ortamda yapay zekâ tabanlı kimlik doğrulama yönteminde, kimlik doğrulama sürecinin doğru bir şekilde sonuçlandırılabilmesi ve saldırganların manipülasyonlarından korunabilmesi için güvenlik açıklarına karşı önlemler alınması gerekmektedir.

Yeni ortaya çıkan DeepFake saldırılarına karşı yüz tanıma sistemleri savunmasızdır ve yüz tanıma sistemlerinin savunma yeteneklerinin DeepFake saldırılarına karşı artırılması gerekmektedir. Çoğu yüz tanıma sistemi, anti-DeepFake tespitlerini içermemektedir. Anti-DeepFake tespiti içeren sistemlerin ise hizmet sağlayıcılar tarafından farklı amaçlar göz önünde bulundurularak geliştirilmiş olması yalnızca belirli türde DeepFake saldırılarına karşı savunma uygulayabilmelerine neden olmaktadır. Dolayısıyla, çok çeşitli yöntemler kullanılarak gerçekleştirilen DeepFake yöntemleri için genel bir savunma henüz sağlanamamış olup bu hususta çalışmalar gerçekleştirilmesi önem arz etmektedir.

Elektronik ortamda yapay zekâ tabanlı kimlik doğrulama süreçlerinde karşılaşılabilecek DeepFake saldırıları için kurcalamaya karşı korumalı donanım ve anti-DeepFake çözümlerinin kullanılması, DeepFake teknolojileri geliştikçe anti-DeepFake tekniklerinin güçlendirilmesi ve DeepFake teknolojilerinin kötü amaçlı kullanımının önüne geçilebilmesi için uluslararası geçerli standartların ve düzenlemelerin geliştirilmesi gerekmektedir.

Yeni gelişen ve uygulanmaya başlayan bir teknolojik gelişmenin kullanımına ilişkin belirli standartların olmaması hem ülke içinde hem de uluslararası alanda birlikte çalışabilirlik esaslarında uyumsuzluklar yaşanmasına neden olabilmektedir. Aynı şekilde, vatandaşların erişimine sunulmuş olan hizmetlere entegre edilen yeni teknolojik gelişmelerin kullanımı ve hizmet sunumu ile ilgili denetim faaliyetlerinin belirlenebilmesi için de bu teknolojilere ilişkin regülasyon çalışmalarının yapılması zorunluluk arz etmektedir.

Saldırı senaryolarının her geçen gün hızlı bir şekilde artırmasından dolayı, dijital dünyada daha fazla standart, sertifikasyon ve test yönteminin ortaya çıkması beklenmektedir. Dolayısıyla, yapay zekâ tabanlı kimlik doğrulama süreçleri için bugün itibariyle belirlenmiş bir standart uygulama bulunmadığı ve bu teknolojinin tüm düzenleyici otoriteler tarafından henüz onay almamış yeni bir teknolojik gelişme olarak sayıldığı göz önünde bulundurulmalıdır. Ayrıca, yapay zekâ tabanlı kimlik doğrulama yöntemlerinde hangi tekniklerin benimseneceği ve hangi kontrollerin uygulanması gerektiği, büyük ölçüde sistemin tasarlandığı kullanım durumlarına ve risk temelli bir yaklaşımı izleyerek sağlaması beklenen güvence düzeyine bağlı olmalıdır.

Bununla birlikte, şirketlerin yüz tanıma ürün ve hizmetlerini geliştirirken verilerin hassasiyetini göz önünde bulundurması, bireylerin açık rızası doğrultusunda yüz tanıma işlemlerinin gerçekleştirilmesi konusunda hassasiyet göstermeleri gerekmektedir.

Sonuç olarak, bir yüz tanıma teknolojisine %100 güvenilmesinin zor olduğu, halen araştırılması ve çözüme kavuşturulması gereken hususların bulunduğu, yapay zekânın yaşam kalitesini iyileştirme potansiyeli olduğu gibi güvenlik açıkları dolayısıyla kötü niyetli saldırganlar tarafından manipülasyonlara uğrama olasılığı, dolayısıyla yapay zekâ sistemlerinin her biri için farklı denetim biçimlerinin mümkün olduğu ve her birinin farklı güçlü veya zayıf yönleri olduğu, yapay zekâya ilişkin yüksek kalitede teknik standartların bulunmaması nedeniyle yeni saldırılara açık olduğu ve yeni güvenlik açıkları ile karşılaşılma ihtimalinin olduğu unutulmamalıdır.

Buna ek olarak, elektronik ortamda yapay zekâ tabanlı kimlik doğrulama süreçlerinde karşılaşılabilecek gerçeğe yakın düzeyde videolar veya sesler oluşturulmasına yarayan DeepFake'in hakaret, gözdağı, gasp, zorbalık ve güvenin zedelenmesi gibi psikolojik zararlarının; kimlik hırsızlığı, dolandırıcılık ve itibar kaybı gibi mali zararlarının ve haber medyasının manipülasyonu, adalet sistemine zarar verilmesi gibi toplumsal zararlarının bulunabileceği hususları da incelenmelidir.

Ayrıca, DeepFake videolarının daha gerçekçi hale getirilmesine neden olan ses klonlama yöntemine ilişkin geliştirme, kullanım, tespit etme ve önlem alma gibi konular da ayrıntılı bir şekilde ele alınmalıdır.

KAYNAKLAR

ABD National Science and Technology Council. (2016, Ekim). The National Artificial Intelligence Research and Development Strategic Plan. https://www.nitrd.gov/pubs/national_ai_rd_strategic_plan.pdf adresinden 1 Temmuz 2024 tarihinde erişildi.

Anderson M.. (2022, Aralık 9). Deepfakes Can Effectively Fool Many Major Facial 'Liveness' APIs. https://www.unite.ai/deepfakes-can-effectively-fool-many-major-facial-liveness-apis/ adresinden 27 Ekim 2024 tarihinde erişildi.

Antispoofing. (2022, Eylül 15). Video Injection Attacks. https://antispoofing.org/video-injection-attacks/ adresinden 16 Eylül 2024 tarihinde erişildi.

Atmaca Y., Bakırcı M. Ç.. (2019, Aralık 1). DeepFake: Yapay Zekâ ve Bilgisayarlar ile Gerçeği Nasıl Bükeriz?. https://evrimagaci.org/deepfake-yapay-zeka-ve-bilgisayarlar-ile-gercegi-nasil-bukeriz-8088 adresinden 29 Eylül 2024 tarihinde erişildi.

AUTHENTICID (2024). Identity Proofing. https://www.authenticid.com/glossary/identity-proofing/, adresinden 21 Aralık 2024 tarihinde erişildi.

AWS. (2023). Yüz tanıma nedir?. https://aws.amazon.com/tr/what-is/facial-recognition/ adresinden 19 Ağustos 2024 tarihinde erişildi.

Berk M. E.. (2020). Dijital Çağın Yeni Tehlikesi "Deepfake. OPUS Uluslararası Toplum Araştırmaları Dergisi, 28(16), 1510-1523. https://doi.org/10.26466/opus.683819.

Bernaciak C., Ross Dominic A.. (2022, Mart 14). How Easy Is It to Make and Detect a Deepfake?. https://insights.sei.cmu.edu/blog/how-easy-is-it-to-make-and-detect-a-deepfake/ adresinden 29 Eylül 2024 tarihinde erişildi.

Carta K., Barral C., El Mrabet N., Mouille S.. (2022). Video Injection Attacks on Remote Digital Identity Verification Solution Using Face Recognition. Proceedings of the 13th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC 2022, 2, 92-97. https://doi.org/10.54808/IMCIC2022.02.92.

Çin Siber Uzay İdaresi. (2022). Provisions on the Administration of Deep Synthesis Internet Information Services. https://www.cac.gov.cn/2022-

12/11/c_1672221949318230.htm.

CyberMag. (2023). Deepfake Videolarının Sayısı Her Yıl %900 Oranında Artıyor!. https://www.cybermagonline.com/deepfake-videolarinin-sayisi-her-yil-900-oraninda-artiyor adresinden 27 Eylül 2024 tarihinde erişildi.

ENISA. (2020). eIDAS Compliant eID Solutions. https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions.

ENISA. (2021). ENISA Remote ID Proofing. https://www.enisa.europa.eu/publications/enisa-report-remote-id-proofing.

ENISA. (2022). ENISA Remote Identity Proofing - Attacks & Countermeasures. https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures.

ENISA. (2023a). Identifying Emerging Cyber Security Threats and Challenges for 2030. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030.

ENISA. (2023b). Artificial Intelligence and Cybersecurity Research. https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research.

Elitaş T.. (2022). Dijital Manipülasyon 'Deepfake' Teknolojisi ve Olmayanın İnandırıcılığı. Hatay Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 19(49), 113-128. https://dergipark.org.tr/tr/pub/hmkusbed/issue/70758/1072624.

ETSI. (2021a). Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects (ETSI TS 119 461 V1.1.1 (2021-07)). https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf.

ETSI. (2021b). Survey of technologies and regulatory requirements for identity proofing for trust service subjects (ETSI TR 119 460 V1.1.1 (2021-02)). https://www.etsi.org/deliver/etsi_tr/119400_119499/119460/01.01.01_60/tr_119460v010101p.pdf

European Parliament. (2023). Artificial Intelligence ACT. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

Facebook Meta. (2020, Haziran 25). Deepfake Detection Challenge Dataset. https://ai.meta.com/datasets/dfdc/ adresinden 25 Ekim 2024 tarihinde erişildi.

Freiberg K.. (2024). Active and passive liveness detection – which one should you use for authentication. https://www.bioid.com/blog/2022/06/active-and-passive-liveness-detection-which-one-to-use-for-authentication/ adresinden 16 Ağustos 2024 tarihinde erişildi.

IDR&D. (2024). How AI Can Prevent a Virtual Camera Injection Attack. https://www.idrnd.ai/how-ai-can-prevent-a-virtual-camera-injection-attack/ adresinden 19 Eylül 2024 tarihinde erişildi.

Interesse G.. (2022, Aralık 20). China to Regulate Deep Synthesis (Deepfake) Technology Starting 2023. https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/ adresinden 11 Ocak 2024 tarihinde erişildi.

Martı C. C., (2021 Ocak 15). Korkunç Bir Siber Tehlike: Deepfake Nedir, Nasıl Çalışır ve Tehlikeleri Nelerdir?. https://listelist.com/deepfake-nedir/ adresinden 23 Aralık 2024 tarihinde erişildi.

NIST. (2017a). Digital Identity Guidelines. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

NIST. (2017b). Digital Identity Guidelines Authentication and Lifecycle Management. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

OECD.AI. (2024). Catalogue of Tools & Metrics for Trustworthy AI. https://oecd.ai/fr/catalogue/metrics adresinden 19 Ağustos 2024 tarihinde erişildi.

Papastratis I.. (2020, Haziran 2). Deepfakes: Face synthesis with GANs and Autoencoders, https://theaisummer.com/deepfakes/ adresinden 28 Eylül 2024 tarihinde erişildi.

STM ThinkTech. (2023, Temmuz 24). Yapay Zekâ ile Üretilen İçerikler Tespit Edilebilir mi?. https://thinktech.stm.com.tr/tr/yapay-zeka-ile-uretilen-icerikler-tespit-edilebilir-mi adresinden 1 Ekim 2024 tarihinde erişildi.

Thales. (2020, Aralık 4). Liveness in biometrics: spoofing attacks and detection. https://www.thalesgroup.com/en/markets/digital-identity-and-se-

curity/government/inspired/liveness-detection adresinden 14 Ağustos 2024 tarihinde erişildi.

Yaman A. U.. (2018). Yüz Tanıma Sistemlerinin Yanıltılmasına Karşı Bir Yöntem: Yüz Videolarında Nabız Tespiti ile Canlılık Doğrulaması [Yüksek Lisans Tezi, Ankara Üniversitesi Fen Bilimleri Enstitüsü]. https://acikbilim.yok.gov.tr/bitstream/handle/20.500.12812/45005/yokAcikBilim_10196903.pdf?sequence=-1&isAllowed=y.

Wang L., Li C., Ji S., Zhang X., Xi Z., Guo S., Wang T.. (2022). Seeing is Living? Rethinking the Security of Facial Liveness Verification in the Deepfake Era. 31st USENIX Security Symposium, 2673-2690. https://www.usenix.org/system/files/sec22-li-changjiang.pdf.