

(God samt skadlig användning av djupfejks och hur de skapas)

Tony Hokkanen

Kandidatavhandling i datateknik

Handledare: Mats Aspnäs

Fakulteten för naturvetenskaper och teknik

Åbo Akademi

(00.00.0000)

Referat

Under de senaste åren har mängden av användare på olika sociala medier ökat drastiskt. På grund av denna ökning är det lättare än någonsin förut att hålla kontakt med nära vänner men också att lära känna nya människor via internet. Sociala medier har tyvärr också lett till att falsk information har blivit lättare att sprida. En sort av farlig falsk information som blivit vanligare under de senaste åren är djupfejks.

Ordet djupfejk härstammar från de engelska orden deep och fake. Där fake översätts som falskt eller oäkta och deep hänvisar till de djupa maskininlärningsmetoder som artificiell intelligens använder. Idén med djupfejks är alltså att ett neuralt nätverk skapar ett ansikte av det bildmaterial det får, som sedan kan klistras in i en annan video.

Då tekniken har blivit vanligare har det utvecklats mer användarvänliga program för att skapa djupfejks, vilket orsakar att det skapas ännu mer falsk information.

I denna avhandling diskuteras det om vad djupfejks är, vilka risker tekniken orsakar samt olika program som kan användas för att skapa djupfejks och hur bra resultat en nybörjare kan få med vissa av dessa program. Dessutom diskuteras det om hur djupfejks kan användas för goda ändamål.

Nyckelord

Djupfejk

Djupinlärning

artificiell intelligens

API

Innehållsförteckning

1	Introduktion	1
2	Djupfejk.....	2
2.1	Vad är djupfakes?	2
2.2	Historia	2
2.3	Hur skapas video djupfejks?	3
2.4	Hur skapas röst djupfejks?	4
2.5	Djupfejkprogram	5
2.5.1	Telefonapplikationer.....	6
2.5.2	Program på Internet.....	8
3	Risker med djupfejk.....	11
3.1	Djupfejk videon.....	11
3.2	Djupfejkning av röst.....	12
4	Positivt med djupfejks	12
4.1	Djupfejk videon.....	12
4.2	Djupfejk röst.....	13
5.	Diskussion och Sammanfattning	14
	Litteraturförteckning.....	15

1 Introduktion

Under de senaste årtionden har tekniken gått drastiskt framåt i vår värld. På internet kan man lätt göra saker som tjugo år sedan skulle ha känts omöjliga. Denna tekniska framgång har hjälpt oss på flera sätt, men teknisk framgång leder inte bara till positiva saker.

Internet har blivit en plats där vissa försöker tjäna pengar på bekostnad av de ovetande. Virus, nätfiske och andra typer av bedrägeri har blivit allt vanligare. Med hjälp av teknisk framgång har det blivit lättare att sprida falska nyheter och annan falsk information. Då vem som helst kan skriva vad de vill på internet är det viktigt att man inte tror på allt man ser eller läser.

Felaktig information är förstås inget nytt, men nuförtiden kan den uppstå i mer avancerade former, och en av nutidens värsta former är djupfejks. Djupfejks, alltså djupt förfalskade videor eller förfalskat tal är bland de farligaste sorterna av spridning av felaktig information.

Djupfejk kan alltså användas för att få det att se ut som om någon gör eller säger något som de aldrig har gjort. Detta kan leda till stora problem på flera olika sätt, det är främst politiker och andra kända personer som blir påverkade av djupfejks. Tanken av att någon kan klistra in ens ansikte på en video var man gör något galet eller ändra på vad man säger på en video känns mycket farlig, och det är hela idén med djupfejks.

Då djupfejks var en ny teknologi så var det främst experter som klarade av att producera dem. När teknologin blev vanligare har det producerats program som har förenklat skapande av djupfejks och nu kan nästan vem som helst skapa djupfejks, även om de inte är lika trovärdiga som de som är gjorda av experter.

Denna avhandling går ut att presentera vad djupfejks är och hur de är producerade samt vilka färdiga program för producering av djupfejks det finns. I avhandlingen undersöks också vilka risker tekniken orsakar men också för vilka goda ändamål djupfejks kan användas.

2 Djupfejk

I detta kapitel kommer det att tas upp vad djupfejk är, historia bakom hur djupfejks uppstod, hur djupfejks skapas och vilka färdiga program för skapande av djupfejks det finns och hur bra de fungerar i en nybörjares händer.

2.1 Vad är djupfakes?

Djupfejk är digitalt manipulerade hyperrealistiska videor eller röster i vilka personen i videon säger och gör saker som aldrig har hänt, djupfejks är skapade med hjälp av olika sorters artificiell intelligens som till exempel maskininlärning och djupinlärning. Djupfejks använder också neurala nätverk som analyserar stora mängder information från vilken den lär sig att imitera personens ansiktsuttryck, beteende och röst.[11][19]

Djupfejkning av ljud är något som också framkommer, med denna teknik kan man få en person att säga vad som helst och då man använder djupfejkning av röst i samband med djupfejk videor kan resultaten bli mycket övertygande. Djupfejks har blivit populära för att kvalitén av förfalskade videorna är bra och för att det finns lättanvända program som både experter och nybörjare inom tekniken kan använda sig av. [14]

Djupfejk riktar sig på sociala medier där falsk information sprids lätt till en stor mängd användare, då användare av sociala media brukar följa med strömmen och sällan kontrollerar om det de läser eller ser är korrekt.[11] Det finns flera olika sätt djupfejk tekniken kan användas, både i goda och onda syften, ännu är det tyvärr vanligare att tekniken används i skadliga syften.[2]

2.2 Historia

Djupfejk blev populärt år 2017 då en Reddit användare publicerade förfalskade videor av kändisar i sexuella situationer skapade med hjälp av djupfejk.[11] Teknologin bakom djupfejks är dock mycket äldre än då den blev populär, vissa experter säger att de verktygen som används i skapande av djupfejks utvecklades redan på slutet av 90-talet. Det är dock svårt att exakt veta när djupfejks skapades för det finns så många olika verktyg som används för skapande av djupfejks och dessa hade helt annorlunda användning då än vad de används för idag. Men år 1997 skapades ett program som man kunde ändra på videor så att personens mun följde det nya ljudet som man satt på videon, och detta kan tänkas vara den första användningen av djupfejk på likadant sätt som tekniken är känt för idag.[18]

I början av 2000-talet till 2017 användes djupfejk en del inom underhållningsindustrin men det skedde inga stora genombrott i användningen av djupfejks före år 2017 då användningen av djupfejks ökade mångfald på grund av Reddit användaren som nämndes tidigare.[18] Efter 2017 har djupfejks använts på många olika sätt och det sägs att mängden av skapade djupfejks fördubblas varje år.[20]

2.3 Hur skapas video djupfejks?

Djupfejk skapas av olika gemenskaper av djupfejk hobbyister, politiska aktörer som till exempel utländska regeringar och aktivister, andra illvilliga aktörer som till exempel bedragare samt legitima aktörer till exempel television företag.[11]

Det finns olika sätt att skapa djupfejks, det sättet som diskuteras i denna avhandling är användning av automatisk kodomvandling. Denna teknik används till exempel i programmet DeepFaceLab som kommer att diskuteras i kapitlet 2.5.2.

Idén med en automatisk omkodning-avkodning är att man har en bild A och en bild B, varefter man med hjälp av omkodning får fram latent ansiktsuttryck från bilderna som kan rekonstrueras med hjälp av avkodning. Dessa omkodare kommunicerar med varandra och delar på informationen de får, denna strategi används så att omkodaren lär sig att hitta små likheter i ansiktena på bilderna som till exempel ögonen eller munnen. För att skapa en djupfejk måste först båda bilderna gå genom denna procedur och efter det kan man skapa en djupfejk med att använda till exempel avkodare B på den Latenta bilden A vilket kommer att producera en bild där ansiktena har blandats ihop.[14] I figuren nedan visas detta.

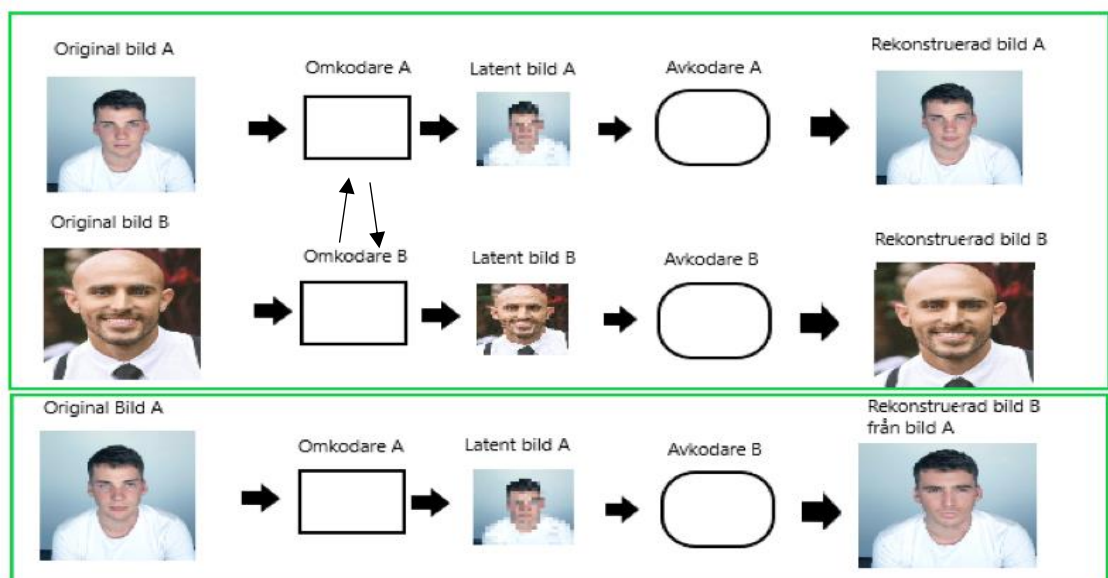


bild 1. Omkodning samt avkodning av bilder för att skapa djupfejks (Hofstra M., Garcia C.)

För att skapa mer avancerade djupfejks kan olika extra program användas vilket leder till att tekniken blir mycket mer avancerad, vissa djupfejk skapare försöker också förbättra sina djupfejks med hjälp av djupfejk detektions program. De sätter sin djupfejk mot ett detektions program och om den blir detekterad så förbättrar de djupfejken och gör detta tills de är nöjda med resultaten. Detta leder till mer övertygande djupfejks men kan också leda till bättre detektion om skaparen delar den information detektorn har lärt sig. [14]

2.4 Hur skapas röst djupfejks?

Röst djupfejks är förfalskade ljud som är skapade eller editerade med hjälp av artificiell intelligens för att verka realistiska. Dessa djupfejks används för att imitera någons röst för olika orsaker, både i goda och onda syften. Det finns olika sätt att skapa ljud djupfejks, dessa är omspels anfall, talsyntes och röstomvandling. [12]

I omspels anfall används inte artificiell intelligens utan tekniken grundar sig på att spela upp inspelat tal av individen som attacken inriktas på, ibland används bara vissa ord av inspelningarna för att skapa nya meningar av de orden som finns inspelat. Dessa anfall kan vara svåra att märka för att rösten är riktig och detta är den enklaste metoden att skapa förfalskat tal.

Talsyntes som är mer känt på engelska som "text-to-speech" kan analysera en skriven text och producera en röst på grund av de regler skaparen har gett som programmet. Denna teknologi är används i olika personliga AI assistenter som till exempel i Apples "Siri" eller Microsofts "Cortana". [12]

Talsyntes kan skapa olika röster med olika accenter och inte bara använda inspelad röst, men för att klara av detta behöver programmet ändå en så kallad "bank" av röster för att sedan skapa den bästa möjliga rösten. För de mest använda språken finns det mycket material att använda för att lära upp dessa program men för mindre språk som till exempel finlandssvenska har det till exempel skapats stora insamlingar av tal för att förbättra röststyrningen av program vilket hänger ihop med talsyntes.[16]

I skapande av talsyntes används några liknande verktyg som i skapande av video djupfejks, dessa är omkodare, avkodare och omvandlare. I skapande av talsyntesen fungerar dessa verktyg lite annorlunda men grundprincipen hålls ganska likadan. Med hjälp av att lära upp det neurala nätverk programmet använder kan talsyntesen skapa en röst som liknar en vald riktig person på endast 5 sekunder, även om inte personens röst använts i utvecklingen av programmet.[16][17]

Röstomvandling är då man använder neuralt nätverk för att ändra en mening som är talad av person A till att låta som om person B skulle ha sagt det. Röstomvandling är effektivt, för att skapa en övertygande röst djupfejk behövs endast en minut inspelat tal av målpersonen.[17]

2.5 Djupfejkprogram

Då djupfejks blev vanligare utvecklades användarvänliga program för skapande av djupfejks. Tanken bakom dessa program kan vara att de bara används på ofarliga sätt, men sanningen är troligen en annan.

Nuförtiden finns det till och med telefonapplikationer för att skapa djupfejk material, dessa brukar vara gjorda för att leka med och inte för att skapa farliga förfälskade videon. De program som man kan hitta på internet och ladda ner på sin dator kan vara mer invecklade. Dessa program kan man skapa farligare djupfejks med men brukar inte vara lika användarvänliga, och ibland behöver man betala för att använda dessa program.



bild 2. testbild för djupfejk program (Hofstra M., unsplash.com)



bild 3. testbild för djupfejk program (Garcia C., unsplash.com)

För att testa de olika programmen kommer testbilderna ovanför att användas. För att skapa en övertygande djupfejk kan det användas flera

hundra bilder, så man kan inte förvänta sig att resultaten med bara en bild kommer att bli lika bra.

Det finns också program för att djupfejka röster men dessa kommer inte att diskuteras i denna avhandling.

2.5.1 Telefonapplikationer

Det finns hundratals olika applikationer för telefonen som använder sig av tekniken bakom djupfejks, men för det mesta är dessa program helt ofarliga och är populära bara för att de är roliga.

Med applikationen Wombo väljer man en bild av sig själv eller från sitt bildgalleri, därefter väljer man en låt och då skapar applikationen en video av personen på bilden, där personens mun rör sig till musikens takt. Detta program orsakar inga farliga problem, och är bara ett sätt att se hur teknologin fungerar. Som man ser på bild 4. kan man lätt märka att videon är förfalskad men ansiktsuttrycken ser ganska bra ut med tanke på att programmet bara använder en enda bild.



bild 4. skärmbilder för resultatet av telefonapplikationen wombo på testbilden 2

Bilderna ovanför är skärmbilder av videon som applikationen har producerat. Applikationen har använts för att få testansiktet att sjunga, videon som applikationen blev ganska dålig bildkvalité, vilket kan vara på grund av att det finns en möjlighet att köpa en premieversion av applikationen som producerar resultat i bättre bildkvalité. På de tagna skärmbilderna ser resultaten bättre ut än på videon som producerades. Applikationens vattenstämpel syns också på bilderna vilket såklart inte stoppar användningen av programmet för att sprida förfalskad information med gör det svårare.

Med telefonapplikationen Reface kan man sätta in sin bild i korta videosnuttar från olika kända filmer och videor. Programmet lyckas inte riktigt med det här och resultatet blir mer av en blandning av det

ursprungliga ansiktet och ansiktet som användaren ger programmet. Men i vissa fall kan resultaten bli överraskande bra.



Bild 5. Testbilden 3 i Reface



bild 6. Originalbilder från "Top Gun"[22]

I bilderna ovanför kan man se att då personen på testbilden liknar original skådespelaren i videon kan resultaten bli mycket bra. Det kunde vara svårt att veta vilken som är de originella bilderna om inte skulle se Refaces vattenstämpel på de förfalskade bilderna. Detta är ett bra exempel av hur effektiv även en enkel djupfejkapplikation kan vara då situationen är perfekt. I de flesta andra fall blir inte resultaten lika bra och man märker lätt att videon är förfalskad.

FaceApp är den mest laddade applikationen av de tre som tas upp i denna avhandling, FaceApp skapar förfalskade bilder i stället för videor som de andra applikationerna. Detta leder till att bildkvalitén är betydligt bättre. Med FaceApp kan man till exempel ändra på miner, hår stil och skägg på bilder, FaceApps föråldrings och föryngrings verktyg är också mycket populärt.



bild 7. Testbilden 2 ändrats med föryngring och föråldringsverktyget i FaceApp

I bilden ovanför har applikationens föryngrings och föråldrings program använts. Även om det inte är möjligt att veta om resultaten är realistiska så verkar resultaten ganska bra och bildkvaliteten är fortfarande bra. Som tidigare nämntes skapar denna applikation bara förfalskade bilder så man kan förvänta sig bättre bildkvalité än de applikationer som skapar videor. FaceApp orsakar troligen inte heller några farliga problem utan tanken är att användarna bara ska ha roligt med applikationen.

2.5.2 Program på Internet

De flesta av de mest övertygande förfalskade videorna är gjorda av program på datorn. Dessa program brukar ha mera verktyg och brukar ta emot mer data vilket leder till bättre resultat. Två av dessa program är Faceswap och DeepFaceLab vilka kommer att diskuteras nedan.

FaceSwap är ett gratis program som är snabbt att installera på datorn, programmet behöver en ganska kraftig dator för att klara av att skapa djupfejks. Som man kan se i skärmbilden nedan är programmet på en helt annan nivå av komplexitet än de telefonapplikationer som tidigare diskuterats.

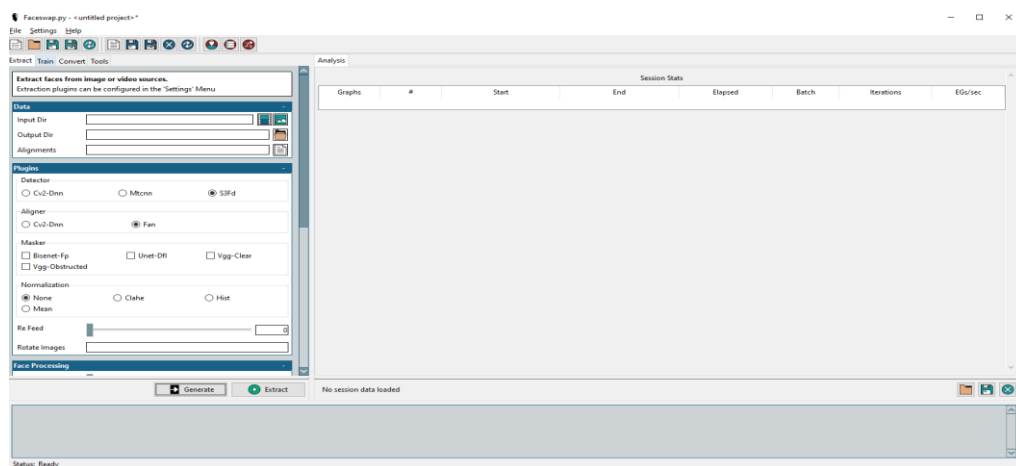


bild 8. Faceswaps meny

Faceswap använder sig av TensorFlow vilket är ett "open source" program för maskininlärning och artificiell intelligens, Keras som också är ett "open

source ” program men för artificiella neurala nätverk och fungerar också som TensorFlows API samt Python som är ett mångsidigt programmeringsspråk. För att skapa en bra djupfejk behövs många verktyg och Faceswap har massor, programmet har så många olika verktyg och inställningar att användningen av programmet är omöjligt utan en nätguide, och även med guiden är programmet inte lätt att använda för en nybörjare. I denna avhandling kommer inte en video djupfejk att skapas utan endast en djupfejk av de två ansiktena som visas i bild 2 och 3.

För att skapa en djupfejk bild med programmet måste man först extrahera ansiktena från både bild 2 och 3 vilket programmet gör automatiskt då man väljer verktyget ”Extract”. För nästa steg måste man ha 25 bilder av ansikte 2 och 25 av ansikte 3, för att tanken var att bara använda dessa två bilder kopierades båda originalbilderna 24 gånger så att programmet fick 25 identiska kopior av båda bilderna. Efter detta sattes kopiorna att träna mot varandra med hjälp av ”train” verktyget, då programmet gjorde detta skapades en modell av ansiktena och ett intervallfoto av ansiktena. Under tiden programmet arbetade var datorn så gott som oanvändbar för programmet använde så mycket av datorns kraft. Programmet ville gå igenom en miljon iterationer av bilderna vilket skulle ha tagit ungefär 55 timmar vilket inte är optimalt så i stället kommer programmet att gå igenom 5000 iterationer vilket tar ungefär 15 minuter. Efter att programmet blev färdigt skapades den en färdig modell och ett intervallfoto som är visas på bild 9.



bild 9. intervallfoto för träningen av Faceswapprogrammet.

Efter detta kan djupfejken äntligen skapas, detta görs med att använda bild 3 som ursprungsbild och modellen som programmet skapade, detta leder till att bild 2 borde sättas på bild 3 och skapa en djupfejk. Resultatet blev dock en besvikelse som man kan se i bilden 10.



bild 10. Djupfejk med Faceswap

Det finns flera orsaker varför resultatet inte kanske blev så bra, den låga mängden iterationer, olika kvalitet på bilderna, låg mängd av bilder eller kanske bara programmet inte tyckte om att det fanns 25 kopior av samma bild vilket möjligtvis ledde till detta resultat.

Det tog ungefär 30 minuter att skapa denna djupfejk, och då användes 25 bilder per ansikte och 5000 iterationer, programmet önskar att få 500–5000 bilder per ansikte och 1 000 000 iterationer för att skapa en video djupfejk vilket skulle öka tiden till flera dygn. Så man märker att skapande av djupfejk är inte så lätt och snabbt som man kanske skulle tro, även med dessa avancerade verktyg.

Deepfacelab är också ett gratis program som inte är lika lätt att installera på en dator. För att datorn skall klara av programmet behövs mycket beräkningskraft vilket betyder att man behöver en mycket kraftig dator för att överhuvudtaget försöka skapa djupfejks. Om man skulle använda en bärbar dator för att använda programmet riskerar man överhettning av nästan alla komponenter i datorn. //Skriv här

Det finns också helt nätbaserade program för skapning av djupfejks, ett av dessa är Deepfakes Web. Dessa program brukar vara lätta att börja använda, oftast bara att registrera sig på websidan, men dessa brukar ha olika avgifter som till exempel molnlagrings tid. Deepfakes Web har exempelvis en molnlagring tids avgift på 3 dollar per timme och därför kommer programmet inte att diskuteras i detalj under denna avhandling. Då ett program använder lika mycket data som dessa blir kostnaden av websidan stor för företaget och därför måste de ha ett annat sätt än annonser för att möjliggöra en inkomst och en vinst. För en nybörjare att skapa en bra djupfejk med dessa program behövs flera timmar arbete, som exempel använde Timothy Lee två veckor och 552 dollar för att skapa en 38 sekunder lång djupfejk video för sin artikel i Arstechnica, och resultatet är ändå inte alls övertygande.[21]

3 Risker med djupfejk

Tyvärr är djupfejk mest känt för negativa orsaker. I detta kapitel diskuteras både djupfejk videon och djupfejkning av röst. Dessa två olika typer av djupfejk kan också fungera bra tillsammans för att en video är mer övertygande då rösten också är förfalskad. I detta kapitel kommer det att diskuteras om hur djupfejk videon och djupfejk röst används för onda ändamål.

3.1 Djupfejk videon

På grund av förfalskade videon blir det svårare för befolkningen att lita på informationen de ser, också journalisters arbete blir svårare då de måste vara säkra om att videon de sett är på riktigt eller inte. Om en journalist skriver om något en person har gjort och det kommer fram att videon var förfalskad, kan konsekvenserna vara stora.

Förfalskade videon kan användas för att förödmjuka andra, kändisar är vanliga mål för videon som har meningen att förödmjuka dem. Flera kända kvinnor har blivit utsatta för förfalskade videor där kvinnornas kläder är borttagna, dessa videor kan leda till stora problem även om det senare kommer fram att kroppen inte är deras på riktigt. Politiker är också vanliga mål för djupfejk, tanken är förmodligen att minska deras popularitet. [7]

En ganska simpel men effektiv användning av djupfejk är att ändra personens mun att röra sig i takt av en mening som är skapad med djupfejkning av röst, då man inte ändrar något annat än munnens rörelser på videon är det svårare att detektera, och med en djupfejkad röst kan man få personen och säga vad man vill. Flera liknande förfalskade videor har skapats av både Ukrainas president Volodymyr Zelenskyy och Rysslands president Vladimir Putin under kriget mellan dessa länder år 2022. [24]

Det värsta med förfalskade videor är att om en person har sett en förfalskad video kommer de kanske inte att få reda på att den är förfalskad, utan de kanske förändrar åsikten om personen för evigt. Den ökande mängden av förfalskade videor har också blivit ett sätt att förklara sig för något man gjort. Om en person på riktigt gjort något dåligt på video och videon sprids, kan personen påstå att videon är förfalskad vilket kan leda till att de slipper undan med det de gjort.

3.2 Djupfejking av röst

Förfalskning av röst används främst i sammanhang med förfalskade videor. Om en video är förfalskad men rösten på personen inte är den rätta märker de flesta snabbt att den är förfalskad, vilket är varför förfalskad röst och video passar bäst ihop. Men förfalskning av endast röst används också för olika brott.

Förfalskning av röst har använts i avancerade brott. En bedragare använde till exempel ett företags chefs röst då bedragaren ringde åt företagets arbetare och lurade dem att flytta 220,000 dollar till bedragarens konto. På grund av att rösten lät så naturlig kunde arbetaren inte tänka sig att det var någon annan än chefen av företaget.[13]

Ett likadant brott hände i 2021 då en arbetare på en bank fick ett samtal av en person som lät identisk till chefen av ett företag som banken tidigare arbetat med och med hjälp av den likande rösten och e-post som var identiska till de som företaget använde slapp rånarna i väg med 35 miljoner dollar.[15]

Vissa kända personer har röster som är kända av miljontals människor känner igen, det känns troligen ganska farligt att någon kan använda deras röster för att säga vad som helst. Vem vet hur många skulle bli lurade av en förfalskad röst då teknologin inte ännu är så känd.

4 Positivt med djupfejks

Då man hör ordet djupfejks tänker de flesta troligen bara på de negativa aspekterna av teknologin, vilket är helt logiskt för det är vad vi hör mest av i nyheterna. Men det finns också möjlighet till positiv användning av djupfejks som möjliggör mycket som kan hjälpa olika industrier och personer. I detta kapitel diskuteras hur djupfejks videon och djupfejks röst kan användas för goda ändamål.

4.1 Djupfejks videon

Djupfejks av videon kan användas för till exempel i filmer för att få skådespelare att se yngre ut i filmer, vilket betyder att i en film där tiden går snabbt framåt kan kännas mer verklig. I stället för att använda en annan skådespelare för att vara huvudpersonen som yngre så kan djupfejks användas för att föryngra skådespelaren, detta är effektivt om det finns mycket filmmaterial av skådespelaren som ung.

Djupfejks har också använts för att "återuppliva" döda skådespelare i filmer. I filmen Fast and Furious 7 använde regissören djupfejks för att ge den tidigare

avlidna Paul Walker en sista stund i filmserien. Regissören använde Walkers bror i filmen för bröderna hade likadan kroppsbyggnad och ändrade ansiktet med hjälp av djupfejk.[23]

Djupfejks kan även användas för att förbättra dubbning i filmer och serier. Ofta är det otrevligt att titta på filmer som är dubbade för att skådespelarnas mun inte rör sig i samma takt som ljudet, men med djupfejk kan munrörelserna ändras att passa ihop med dubbningen i stället för original ljudet, vilket leder till en trevligare erfarenhet för tittarna.[8] Men en även mer avancerad teknik har skapats, en grupp i Indien har skapat en teknik att använda djupfejks för att översätta ljudet från en video på engelska till hindi och på samma gång ändra munrörelserna i videon att passa in med det nya språket. Denna teknik är ännu ny och förstås mycket dyrare och svårare än att bara skapa en översättning eller att dubba filmen men man kan se att möjligheterna inom djupfejk är nästan ändlösa.[25]

I kapitel 2.5.1 kom det också fram att det finns hundratals ofarliga djupfejk baserade applikationer för telefonen som kan sprida glädje till dess användare. Alla dessa ofarliga sätt att använda djupfejks förbättrar konsumenternas erfarenhet men möjliggör också arbetsplatser åt flera duktiga arbetare.

4.2 Djupfejk röst

Sjukdomar och olyckor som orsakar förlust av talförmåga är inte så ovanliga, detta kan kännas hemskt men med djupfejkning av röst är det möjligt att få sin röst tillbaka till en viss grad. Skådespelaren Val Kilmer tappade sin röst på grund av halscancer, men företaget Sonatic lyckades återskapa Kilmers röst med hjälp av Kilmers gamla filmer. Med hjälp av den digitala rösten Sonatic producerade kan Kilmers kommunicera med sin ”egna” röst i viss mån. [4]

Men det är inte endast levande människor vilkas röster kan återställas utan också eventuellt avlidnas röster. Till exempel avlidna musikartisters röster skulle kunna digitaliseras och användas för att skapa nya sånger eller slutföra deras halvfärdiga låtar. Sådan användning av djupfejkning av röst kan troligen väcka många moraliska frågor men dessa är inte det viktiga i denna avhandling.

Djupfejkning av röst är en ganska ny teknologi och användningen är inte ännu så avancerad. Då teknologin utvecklas kommer det troligen många nya sätt hur teknologin kan användas.

5. Diskussion och Sammanfattning

...

Litteraturförteckning

- [1] Adee S. (2020). "What Are Deepfakes and How Are They Created?" *IEEE Spectrum*.
- [2] Sharmin A., Mahmud B.U., (2020). "Deep Insights of Deepfake Technology: A Review." *Dujase*.
- [3] Beebom, (2022). "10 Best Deepfake Apps and Websites You Can Try for Fun." *Beebom*.
- [4] Brown D. (2021). "AI gave Val Kilmer his voice back. But critics worry the technology could be misused." *The Washington Post*.
- [5] Caporusso N. (2021). "Deepfakes for the Good: A beneficial Application of Contentious Artificial Intelligence Technology." *ResearchGate*.
- [6] Farish K. (2020). "Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of the deepfake." *Journal of Intellectual Property Law & Practice*.
- [7] Greengard S. (2020). "Will Deepfakes Do Deep Damage?" *Communications of the ACM*, 17-19.
- [8] Hsu J. (2021). "AI Modifies Actor Performances for Flawless Dubbing". *IEEE Spectrum*.
- [9] Muna M. (2020). "Technological Arming: Is Deepfake The Next Digital Weapon?" *ResearchGate*.
- [10] Usukhbayar B. (2020). "Deepfake Videos: The future of entertainment." *ResearchGate*.
- [11] Westerlund M. (2019). "The Emergence of Deepfake Technology: A Review." *Technology Innovation Management Review*.
- [12] Khajani Z., Watson G., Janeja V.P., (2021). "How Deep are the Fakes? Focusing on Audio Deepfake: A Survey." *University of Maryland, Baltimore County*.
- [13] Stupp C., (2019). "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case" *The Wall Street Journal*.
- [14] Nguyen T., Nguyen Q., Nguyen D., Nguyen D., Huynh-The T., Nahavandi S., Nguyen T., Pham Q., Nguyen C. (2019). "Deep Learning for Deepfakes Creation and Detection: A Survey." *ResearchGate*
- [15] Urian B. (2021). "Bank Robbers Used Deepfake Voice for \$35 Million Heist AI-Enhanced Voice Simulation Used" *Techtimes*
- [16] Villanen F.(2021). "Vill du att röststyrningen ska fungera på finlandssvenska? Kom med och donera prat" *Svenska. YLE*
- [17] Jia Y., Zhang Y., Weiss R., Wang Q., Shen J., Ren F., Chen Z., Nguyen P., Pang R., Moreno I., Wu Y., (2018). "Transfer Learning from Speaker Verification to Multispeaker Text-TO-Speech Synthesis" *Advances In Neural Information Processing Systems* 31 s. 4485-4495
- [18] Arnold. (2020). "Deepfake History: When was Deepfake Technology Invented?" *Deepfakenow*
- [19] Huijstee M., Boheemen P., Das D., Nierling L., Jahnel J., Karaboga M., Fatun M., Kool L., Gerritsen J., (2021). "Tackling deepfakes in European policy" *European Parliament*
- [20] Chen H., Rouhsedaghat M., Ghani H., Hu S., You S., Kuo J., (2021). "DefakeHop: A Light-Weight High-Performance Deepfake Detector." *ResearchGate*
- [21] Lee T. (2019). "I created my own deepfake-it took two weeks and cost \$552" *Arstechnica*
- [22] Scott J. (1986). "Top Gun" *TM & Paramount Pictures*<https://www.youtube.com/watch?v=01nS19OOD-U>
- [23] Schaeffer S. (2021). "How Furious 7 Finished Paul Walker's Scenes After His Death" *Screenrant*

[24] Wakefield J. (2022). “Deepfake presidents used in Russia-Ukraine war” *BBC*

[25] Prajwal R., Mukhopadhyay R., Philip J., Jha A., Namboodiri V., Jawahar C., (2019). “Towards Automatic Face-to-Face Translation” *Proceedings of the 27th ACM International Conference on Multimedia s.1428-1436*