Biblios
ISSN 1562-4730 (online)

“Deepfake” como ferramenta de manipulação e disseminação de “fakenews” em formato de vídeo nas redes sociais

Cristiane Pantoja De Moraes
Universidade Federal do Pará, Brasil

REVIEW

Resumo

Objetivo. A pesquisa a seguir tem como objetivo analisar os novos conteúdos de disseminação de informações falsas, assim buscando conceituar o que seriam as “deepfake” e as “fakenews” e as consequências dessas manipulações de imagem e veiculação de noticias.
Metodo. Desenvolveu-se uma pesquisa exploratória com levantamento bibliográfico de materiais previamente publicados, como artigos de periódicos científicos, em que foi realiza uma revisão de literatura apropriada de maneira a esclarecer e apresentar o assunto sobre as “deepfakes” ainda pouco conhecida, além disso, apresentar de que maneira ela é criada, manipulada a ponto de se dissemina de mananeira desenfreada frente às redes sociais.
Resultados. Sabe-se que hoje os softwares e aplicativos para smatphones proporcionam, de modo muito hábil, que usuários manipulem imagem com extrema facilidade, os chamados fakeApp,que são ferramentas que permitem alteração e manipulação de imagens de maneira que não deixem pistas visuais de sua alteração, podendo ser indistinguíveis aos autênticos. Exemplo do resultado destas manipulações é a “deepfake”, é a técnica que substitui o rosto de uma pessoa por outra em um vídeo, no panorama atual é comum visualizar vídeos falsos, o que geram as “fakenews”, ou notícias falsas, muito veiculadas nas redes sociais e que cabem por ganhar certa credibilidade devido à dificuldade de distinguir a veracidade na imagem ali mostrada, tão quão são imperceptíveis as marcas de adulteração. O que facilita a produção das “fakenews”, é que qualquer usuário com conhecimento limitado de programação e pouca aprendizagem tecnológica pode criar “deepfakes” e esse tipo de produção tem desencadeado desafios aos profissionais forenses, que ainda encontram significativa diferença entre as “deepfakes” e os vídeos autênticos.

Palavras-chave:
Deepfake; Fakenews; Manipulação de imagem.

“Deepfake” as a tool for manipulating and disseminating “fakenews” in video format on social networks

Abstract

Objective. The research to proceed has as objective analyzes the new contents of spread of false information, like this looking for to consider what would be the “deepfake” and the “fakenews” and the consequences of those image manipulations and veiculação of you announce.
Method. To develop an exploratory research with bibliographic survey of published materials, such as articles from scientific journals, in which a literature review was carried out in an easy way to clarify and present the subject of deepfakes still little known, and also presented that The way it is created, it manipulates a point of unbridled maneuver in front of social networks.
Results. It is known that today the software and applications for smatphones provide, very skillfully, that users manipulate images with extreme ease, the so-called fakeApp, which are tools that allow alteration and manipulation of images in a way that do not leave visual clues of their alteration, and may be indistinguishable from authentic ones. An example of the result of these manipulations is the “deepfake”, is the technique that replaces the face of one person by another in a video, in the current panorama it is common to visualize fake videos, which generate fakenews, or fake news, widely disseminated on social networks and that fit for gaining some credibility due to the difficulty of distinguishing the veracity in the image shown there, as much as the adulteration marks are imperceptible. What facilitates the production of “fakenews” is that any user with limited programming knowledge and little technological learning can create “deepfakes,” and this type of production has triggered challenges for legal professionals, who still find a significant difference between “deepfakes” and authentic videos.

Keywords:
Deepfake; Fakenews; Image manipulation.

1 Introdução

Os vídeos conhecidos como "Deepfake" oferecem a capacidade de trocar o rosto de uma pessoa por outra em um videoclipe ou imagem, essa tecnologia criada para vídeos foi projetada para melhorar continuamente seu desempenho, principalmente para aprimora os vídeos e cria os vídeos falsos que imitar as expressões faciais, gestos, voz e variações do indivíduo, tornando-os cada vez mais realistas (Maras & Alexandrou, 2019, Ngiam et al. 2011).

Este trabalho tem como objetivo fazer uma análise dos novos conteúdos digitais no âmbito da disseminação de falsas informações ou como são comumente conhecidas, as "fakenews", em formato de vídeo as chamadas "deepfake" nas redes sociais, uma vez que elas ganham rapidamente grande repercussão ao serem compartilhadas pelos usuários, viralizando na Internet. Com base nisso, através da literatura disponível sobre este tema, procurou-se discutir o que é "deepfake" e "fake news", no contexto da produção e disseminação, bem como seu papel como ferramenta de manipulação das notícias no ciberespaço.

> [...] as notícias falsas ficaram em evidência. Sintetizando e simplificando a percepção geral: a epidemia de notícias falsas fez com que os eleitores e a opinião pública tomassem decisões equivocadas, baseadas na emoção e em crenças pessoais, ao invés de em fatos objetivos (Genesini, 2018, p.47).

De acordo com Bunk et al. (2017), o número de imagens digitais tem crescido exponencialmente com o advento de novas câmeras, smartphones e tablets. As mídias sociais, como Facebook, Instagram e Twitter contribuíram ainda mais para a sua distribuição. Dessa forma, as ferramentas para manipular digitalmente imagens evoluíram gradativamente e os softwares e aplicativos para smartphones tornam-se muito trivial para os usuários que manejam facilmente imagens.

As mudanças que ocorrem no mundo tecnológico, principalmente na manipulação de imagem e vídeos, geraram um campo para a criação de ferramentas modernas e livres, muitas vezes de acessos facilmente disponível, impulsionando o mercado e o paradigma quando se tratam de estruturas modernas de adulteração de imagem e vídeos que antes eram de domínio restrito para indivíduos treinados e hoje pode ser amplamente acessível a qualquer pessoa que tenha um computador, desktop e até um smartphone que contenham aplicativos como *FakeApp*[i].

O reconhecimento facial é uma tecnologia biométrica largamente utilizada porque é mais conveniente de usar do que outras abordagens biométricas, essa tecnologia de reconhecimento facial, tem se desenvolvido rapidamente nos últimos anos sendo uma das mais convenientes em comparação com outros métodos. No entanto, sistemas de biometria[ii] para reconhecimento facial são ingênuos e não suportam qualquer tipo de detecção podendo ser facilmente falsificado usando apenas uma fotografia. Essa detecção de rosto é uma questão-chave no campo dos sistemas de segurança que utilizam câmeras, pois, infelizmente, existem falhas de impressão e borrão geral da imagem. Mas com o desenvolvimento de dispositivos de exibição e tecnologia de captura de imagens, é possível reproduzir imagens de rostos semelhantes a rostos reais, o que gera número significativo de ataques usando uma fotografia ou vídeo exibido em uma tela (Miyoung & Youngsook, 2017).

A crescente sofisticação da tecnologia de câmera móvel e o alcance veloz das mídias sociais e mídia fizeram a criação e propagação de vídeos manipulados mais convincentes do que nunca. No que diz respeito aos números de vídeos falsos e seus graus de e sofisticação, o tempo de fabricação e manipulação destes tem diminuído significativamente nos últimos anos, graças à acessibilidade e ao grande volume e poder de computação e aplicativos fakeapp, e isso inclui também o crescimento do aprendizado em relação às máquinas e a visão mais detalhista de qualquer pessoa, que elimina a necessidade de um profissional (Li & Lyu, 2018; Maras & Alexandrou, 2018).

Hoje, as imagens digitais podem ser facilmente manipuladas e alteradas, as falsificações digitais, muitas vezes não deixam pistas visuais de alteração, podendo ser indistinguíveis aos autênticos (Popescu & Farid, 2005).
Nas últimas décadas, a popularização dos smartphones e o crescimento das redes sociais fizeram as imagens e vídeos digitais objetos tão comuns, de acordo com vários relatórios, quase dois bilhões de fotos são enviadas todos os dias na internet, entretanto surgiu um aumento de técnicas para alterar o conteúdo da imagem, usando software de edição, o que gerou um campo de investigação forense digital dedicado à detecção de falsificações de imagem, a fim de regular a circulação tais conteúdos (Afchar, Nozick & Yamagishi, 2018).

A propagação de desinformação através de imagens e vídeos se tornou mais realistas, o que gerou um grande problema na atualidade, exigindo métodos de detecção de manipulação potentes, que apesar do esforço predominante na área, e a detecção da manipulação rosto adulterados em vídeos. A utilização da aprendizagem profunda que têm se mostrado eficazes em explorar a informação temporal a partir de fluxos de imagem em vários domínios. Através de técnicas de pré-processamento de rostos através de extensiva experimentação para obter

um desempenho satisfatoris nos parâmetros que se referema manipulação faciais de disponíveis publicamente, mas espeficifamente na em detectar Deepfake adulterado em vídeos (Sabir et al, 2019).

2 Metodologia

Desenvolveu-se uma pesquisa exploratória com levantamento bibliográfico de materiais publicados, como artigos de periódicos científicos, em que foi realiza uma revisão de literatura apropriada de maneira a esclarecer e apresentar o assunto sobre os "deepfakes" ainda pouco conhecida, além disso, esclarecer de que maneira esta nova fakenews foi criada, manipulando notícias falsas a ponto de se dissemina de uma maneira desenfreada frente às redes sociais.

3 O que é "Deepfake"

"Deepfake" é uma técnica que visa substituir o rosto de uma pessoa por outra em um vídeo. Em questão de datas, o primeiro ocorreu em Outono de 2017 utilizado para gerar conteúdos adultos. Posteriormente, essa técnica foi melhorada por uma pequena comunidade para criar nomeadamente uma aplicação chamada *FakeApp.* O processo para gerar *deepfake* consiste em imagens que reúnem rostos alinhados de duas pessoas diferentes, nas quais há a reconstrução do rosto de uma em conjunto de dados de imagens faciais da outras e se auto-codifica para então reconstruir rostos com as imagens faciais. Na prática, os resultados são impressionantes, o que explica a popularidade da técnica. O último passo é levar o vídeo ao alvo, extrair e alinhar a face do alvo a partir de cada quadro, utilizando software ou aplicativos *FaceApp*[iii] para gerar outra face com a mesma iluminação e expressão, e então fundir de volta no vídeo (Afchar et al., 2018).

Atualmente, de acordo com Korshunov e Marcel (2018); Güera e Delp (2018), o *FaceApp* uma forma de *FakeApp* trata-se de uma ferramenta para smartfones que pode gerar automaticamente rostos em fotografias o que torna a imagem altamente realista, permitindo a mudança de rosto, cabelo, sexo, idade e muitos outros detalhes usando apenas o telefone móvel.

Os chamados *deepfakes* são a mais nova forma de manipulação de mídia digital, atualmente existem diversas ferramentas de softwares livres aperfeiçoados em aprendizagem de máquinas que criam facilmente rostos em vídeos deixando poucos resquícios de manipulação.

Exemplo de uma imagem (esquerda) ao ser manipulado (à direita), utilizando a técnica *deepfake*. Note-se que a face trocada não apresenta a expressividade do original.

Figura 1: Exemplo de manipulação com a técnica deepfake

Fonte: De (Afchar, Nozick & Yamagishi, 2018).

3.1 Como o "Deepfake" pode manipular e disseminar as "Fake news" nas redes sociais

No panorama atual, é comum visualizar vídeos falsos e, por sinal, são totalmente realistas, o que os tornam perigosos pessoalmente como politicamente, às vezes são utilizados para falsas promoções, chantagens e até desmoralização pessoal.

Maras & Alexandrou (2019) comentam que em uma sociedade em que as informações são consumidas e reproduzidas rapidamente, seja por meio das mídias sociais e outros meios de informação, os Deepfakes pode gerar

efeitos prejudiciais sobre aqueles que são direcionados nos vídeos, posi estes geralmente permanecem on-line por longos períodos e podem ser transferidos por diferentes fontes de informação, mesmo quando removidos podem vezes até reaparecem e ser ser usados e pornografia, intimidação, evidência em vídeo, sabotagem política, propaganda, em notícias falsas ou fakenews, que consiste na desinformação e propaganda que distorcem notícias e fatos reais, substituindo o conhecimento por imagens e informações falsas.

> O novo é que estamos em uma nova era turbinada pela internet e pelas redes sociais, em que o crescimento é viral e o efeito, exponencialmente explosivo. O novo é o Facebook, o Google e o Twitter, não a tentativa de contar mentiras ou falsificar informações, o que sempre existiu na história do mundo (Genesini, 2018, p.46).

Com o advento das redes sociais, aproliferação de tal conteúdo pode ser imcomparável e pode potencialmente agravar os problemas relacionados com as teorias de desinformação e de conspiração (Hasan & Salah, 2019).

É comum nos divertimos usando o recurso *faceswap*[iv] em aplicativos de celulares, uma opção que literalmente faz a trocar rostos, mesmo que consista em mudar de rostos com nossos amigos ou parecer como uma celebridade, essa tecnologia é frequentemente usada de maneira desagradável. No entanto, o reconhecimento facial tornou-se um pesadelo para alguns famosos com o surgimento dos deepfake, permitindo que os usuários criem vídeos com pessoas usando a aparência destes.

Frequentemente essa tecnologia tem sido usada para criar vídeos pornográficos falsos de celebridades causando imagens assustadoras, uma vez que é muito além de uma simples "troca de rostos", como as utilizadas nos aplicativos de celulares, isso acontece com deepfake, pois é um conjunto de técnicas utilizadas para sintetizar novos produtos visuais, por exemplo, substituindo rostos nos originais (Floridi, Korshunov & Marcel, 2018).

De acordo com Korshunov e Marcel (2018) são de grande preocupação pública a respeito dos deepfakes, existem atualmente software de código aberto acessível e aplicativos utilizados para a troca de rosto, o que gera uma grandes quantidade de vídeos sinteticamente manipulados e distribuídos na mídias sociais e notícias, o que representa um significante desafio técnico para detecção e filtragem de tal conteúdo.

Já não é de hoje as várias tentativas para a troca de rosto. Conforme Güera e Delp, (2018), explicam que, por volta de 1865, foram encontrados na litografia os traços do presidente dos Estados Unidos Abraham Lincoln de acordo com a figura a seguir, assim como utilização de *fakeapp* para a produção de *deefakes*.

Abaixo o exemplo de troca da cabeça do Presidente Lincoln com o corpo do político John Calhoun, criadas no século XIX (esquerda) e ferramentas modernas como, por exemplo, fakeapp viraram mais fácil para qualquer se

Figura 2: exemplo de troca de rostos por meio da *deepfake*

Fonte: De (Afchar, Nozick & Yamagishi, 2018).

O que distingue deepfakes de outras técnicas de manipulação de vídeo é, primeiramente, o seu potencial de resultados fotorrealista, com imagens em que os vídeos resultantes podem ser extremamente convincentes. Em segundo lugar, a disponibilidade da técnica para leigos em um aplicativo chamado fakeapp, que se trata uma in-

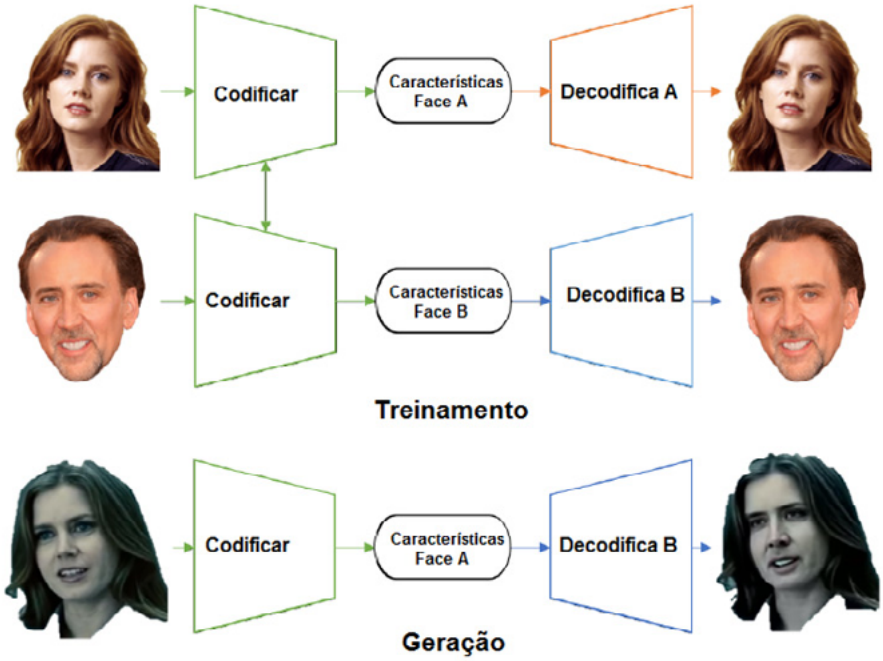
No 79 (2020) • http://biblios.pitt.edu/ • DOI 10.5195/biblios.2020.864

terface lançada e desenvolvida em torno do algoritmo *deepfake*, que permite que os usuários com conhecimento limitado de programação e pouca aprendizagem em tecnologia possam criar *deepfakes.*

Segundo Koopman, Macarulla Rodriguez e Geradts (2018) essa combinação de resultados fotorrealista é facilmente utilizada gera um aumento na necessidade de criar métodos autenticação para detecção de manipulação em deepfake, o que tem gerado um problema na atualidade das "notícias falsas", as chamadas *"fake news"*, que vão se tornando mais relevante também para os jornalistas em vídeo, hospedagem de sites e usuários de mídia social".

O que faz deepfakes ser facimelte manipulda poies é possível é encontrando uma maneira em que ambas as faces a serem codificados nos mesmos recursos. Isto é, existem duas faces que compartilham o mesmo codificador, são descodificadas fazendo assim fazer um novo rosto através da junção de faces demostrada (em baixo).

Figura 3: Como ocorre formação e geração durante a criação de um vídeo deepfake



Fonte: (Guera, D.& Delp, E. J., 2018).

Hoje, o perigo de notícias falsas é amplamente reconhecido num contexto em que milhões de horas de conteúdo de vídeo são vistos diariamente em redes sociais, a propagação de vídeos falsificados aumentou o nível de preocupação. Por mais que melhorias sejam feitas para detecção de imagem falsificada, vídeo digital manipulados, o desvendamento continua a seu uma tarefa difícil.

Com os aparecimentos dos deepfake como cita Korshunov e Marcel (2018); Güera e Delp (2018), ferramentas que geram os deepfakes de vídeos têm sido amplamente utilizadas para criar falsas notícias de celebridades associados às pornografias ou até mesmo vídeos de vingança. Alguns sites como o Twitter já proibiram esse tipo de vídeos, embora a natureza desses vídeos quase que realista, torna-se alvo para gerar matérias de conteúdos ilícitos, falsos, pornográficos e maliciosos, utilizados até para criar tensão política e estão sendo alvos da atenção das entidades governamentais.

3.2 Como detectar os "Deepfake"

De acordo com Tan, Li, Liu e Jiang (2010) é comum que os dados faciais sejam roubados ou duplicados em um sistema de reconhecimento de face. Isto porque na internet, uma ou mais fotografias de um usuário pode ser facilmente obtida, sem contato físico o usuário através de download via internet ou simplesmente captura-los usando uma câmera. Este sistema de reconhecimento facial baseado em imagens 2D pode ser facilmente manipulado por truques considerados bem simples, e que na verdade, é uma tarefa muito desafiadora para em que os esforço maior vem na pesquisa de reconhecimento facial que no momento atual estaá focada mais na imagem correspondente do sistema sem se importar se o rosto combinado é de um ser humano.

Recentemente, o reconhecimento de rosto tornou-se cada vez mais importante devido aos rápidos avanços em dispositivos de captura de imagem (por exemplo, câmeras de vigilância e câmera em celulares), onde a disponibilidade de um número muito grande de imagens de rosto na internet, e as crescentes demandas por maior segurança (Li & Jain, 2011 como citado em Miyoung & Youngsook, 2017).

Os autores Korshunov e Marcel (2018) comentam que se considerarmos os vários sistemas de detecção Deepfake, incluindo o sistema que utiliza dados de áudio-visual para detecção de inconsistências entre movimentos labiais e discurso de áudio,assim como, diversas variações nos sistemas baseados em imagem têm como objectivo distinguir os vídeos genuínos, onde o movimento da fala é sincronizado, no vídeo que foi modificado, e esses movimentos dos lábios e áudio, pode não ser necessariamente o discurso original.

A tecnologia faceswap é um programa deepfake em que se usa pesquisa de imagens na internet, explorando sites de mídia social, e depois, por conta própria, insere dados para substituir os rostos em vídeos quase que perfeitamente. O programa não precisa de nenhuma supervisão humana, seu processo de aprendizagem é independente e continua a melhorar o processo de forma autônoma. Qualquer pessoa pode criar vídeos pornográficos estrelados por celebridades, políticos, amigos ou inimigos (Cuthbertson, 2018 como citado em Maras & Alexandrou, 2018).

Alegações de "notícias falsas" já são tão comuns, tanto que a vítima de um vídeo falsificado pode não ser capaz de estabelecer a credibilidade ao afirmar que tenham sido falsificados, pois existe uma abundância de ferramentas sofisticadas para a detecção de falsificação de imagem. São susceptíveis de ser desenvolvidos, já que a demanda por eles tem aumentando (Floridi, 2018).

Conforme Koopman et al. (2018), o algoritmo responsável por gerar o deepfake permite que um usuário possa mudar o rosto de um ator em um vídeo com o de um ator diferente de uma forma fotorrealista, isso desencadeia desafios aos profissionais forenses com relação à confiabilidade das provas de vídeo. Os testes realizados quanto à sua eficácia na detecção de manipulação de vídeo deepfake ainda mostram diferença significativa entre vídeos autênticos e "Deepfakes". Ultimamente, as provas fotográficas e de vídeo são comumente usados nas investigações tribunal e da polícia, que eram vistas como confiáveis de provas, no entanto, essas amostras de vídeo estão tornando-se potencialmente pouco viáveis e provavelmente serão necessários resquícios nesses vídeos, pois ao serem examinados cautelosamente, sempre deixam vestígios de adulteração antes de serem considerados admissíveis para qualquer tribunal.

3.3 Aprendizagem profunda na detecção de Deepfakes

A aprendizagem profunda ou Deep Learning são redes neurais artificiais se tornarm um campo de pesquisa incrivelmente atraente no ramo de reconhecimento de objetos que ulrapassaram a capacidade humana que vai desde reconhecimento de fala, geração algorítmica de rostos e paisagens, até mesmo a reconstrução de estímulos visuais a partir de gravações. O sucesso dessas disso se dá utilizando a aprendizagem profunda para análise de dados modelandos aspectos do processamento (Sullivan, 2019).

A Representação de aprendizagem é um conjunto de métodos que permite que uma máquina a ser alimente de dados em bruto para a detecção automática, e essas representações são necessárias para a detecção ou classificação dos aprendizagem profunda com vários níveis de representação (LeCun, Bengio & Hinton, 2015).

Vídeos Deepfake utilizam a técnicas de aprendizagem profundas para conseguir rosto troca mostras de imagens de vídeo. Quanto maior o número de amostras, a mais realista são os seus resultados (Hasan & SALAH,2019).

Antes do surgimento da aprendizagem profunda, invasores maliciosos criavam manualmente mídia falsificada usando utilizando softwares como Adobe Photoshop ou GIMP2, tornando o processo tedioso, mas hoje, o cenário se transformou drasticamente, anteriormente o aprendizado de máquina swe modificou e as ferramentas passaram a ajudara o usuário na criação de conteúdo inovadores, o que atualmente fazem com que as aquinas usem ferramentas que criam conteúdo sem intervenção manual. O realismo alcançado pelos componentes da aprendizagem automática são tão elevados, que mesmo aos olhos dos seres humanos exitem dificaldades em distinguir se uma face é capiturada naturalmente com uma câmara ou se é artificialmente produzida. (Sabir et al, 2019).

No mundo dos falsos deepfakes e a aprendizage profunda usam o aprendizado de máquina e inteligência artificial e processamento de imagem para criar vídeos retratando pessoas dizendo ou fazendo coisas que jamais

disseram ou fizeram (Joseph, 2019; Hasan & Salah, 2019). Os vídeos do Deepfake são criados usando tecnologia baseada na inteligência artificial (IA), em que modelos computacionais de comportamento humano apresentam processos de pensamento projetados para atuar de maneira lógica e inteligente como a simulação de um comportamento humano (Maras, 2017).

De acordo com LeCun, Bengio & Hinton (2015) a aprendizagem profunda aceita que os modelos computacionais que são compostas de camadas múltiplas de processamento que aprende a representa dados com vários níveis de abstração, métodos estes que melhoraram dramaticamente o estado da arte em se tratando do reconhecimento de voz, reconhecimento e detecção de objetos visuais. Essa aprendizagem profunda trouxe muitos avanços no processamento de imagens, vídeo. Em pesquisas na web para filtragem de conteúdo,que esta cada vez mais presente, produtos de consumo como câmeras e smartphones, em que os sistemas de aprendizado dessas máquinas são usados para identificar objetos em imagens, produtos com diversos interesses para os usuários, e a seleção de busca de produtos para determinado público é selecionado através de resultados relevantes de pesquisa e isso esta cada vez mais frequente,e essas aplicações fazem uso de uma classe de técnicas chamadas aprendizagem profunda.

Durante os últimos anos, métodos de aprendizagem profunda foi um sucesso empregado nas perícias de imagens digitais. Usar a aprendizagem profunda para detectar imagens, propõe uma rede para detectar o alvo da falsificação distinguindo gráficos de computador, executa muito bem pelos profissionais forenses digitais (Miyoung & Youngsook, 2017).

Com a ascensão da Inteligência Artificial (AI) e técnicas de aprendizagem profunda, abriram o caminho para a produção de deepfake vídeos, os conteúdos digitais falsos têm proliferado nos últimos anos. Filmagens falsas, imagens, áudios e vídeos (conhecida como deepfakes) pode ser um fenômeno assustador e perigoso e pode ter o potencial de alterar a verdade e gerando desconfiança e gerando uma falsa realidade (Hasan & Salah, 2019).

Em falsificação de vídeo é outra grande ameaça, que os sistemas de reconhecimento enfrentam, pois são muito semelhantes a um rosto ao vivo. Devido a isso, as fotografias e vídeos são os mais comuns utilizados na manipulação de imagem, pois estão facilmente disponíves na internet.

4 Resultados

Os *"Deepfakes"*, quando comparadas a informações não rotuladas como "notícias falsas" ou *Fakenews*, causam impactos quando são descobertas e um dos desafios da atualidade é rastrear "notícias falsas" na batalha contínua contra a desinformação.

Em seguida, se analisamos a relação entre a manipulação e disseminação de notícias falsas, as duas são reconhecidas como desinformação, haja vista que os usuários estão sujeitos a todo e qualquer tipo de imagem e vídeos compartilhados todos os dias nas redes sociais, fatos que mostram aumento nos resultados da polarização de *"fakenews"* em que usuários associam a palavras-chave e *hashtags*[v] em notícias falsas, sem ao menos buscar a verdadeira fonte ou fonte confiável ao compartilhar a informação. O impacto dessa nova descoberta dos deepfake veio como desafio para rastrear "notícias falsas" no intuito de diminuir a propagação destas de acordo com peritos digitais.

As notícias apontaram a necessidade de manter um firme controle incidente sobre as notícias falsas, pois elas podem colocar em risco a liberdade de expressão, a honra das pessoas e o próprio processo democrático de um país. Foi possível notar, ainda, que para se combate as *fakenews*, é obrigatório o respeito à liberdade de expressão, e contar com a cooperação e a ética dos usuários em compartilhar a notícia publicada.

5 Conclusões

Hodiernamente, o perigo da adulteração facial, ocasionado pela mudança no vídeo ainda não são amplamente reconhecidos pela população. Apesar de existirem produtos para detectar tais falsificações de forma eficiente e com um baixo custo computacional, muitas pessoas ainda desenformadas disseminam todo e qualquer tipo de vídeo sem se importar com sua veracidade ou fonte o que ocasiona uma disseminação desencadeada de falsas notícias que são rapidamente espalhadas em questão de segundos na internet.

Referências

Afchar, D., Nozick, V., & Yamagishi, J. (2018). MesoNet: A compact facial video forgery detection network. arXiv:1809.00888v1 [cs.CV] 4 Sep 2018. Recuperado de https://arxiv.org/abs/1809.00888.

Bunk, J. , Bappy, J. , Mohammed, T. , Nataraj, L. , Flenner, A. , Manjunath, B. , Chandrasekaran,S., … Peterson, L. (2017). Detection and localization of image forgeries using resampling features and deep learning. arXiv:1707.00433v1 [cs.CV] 3 Jul 2017. Recuperado de https://arxiv.org/abs/1707.00433.

Floridi, F. (2018). Artificial Intelligence, Deepfakes and a Future of Ectype. *Springer Netherlands*. 31, 317-321. doi:10.1007/s13347-018-0325-3

Genesini, S. (2018). A pós-verdade é uma notícia falsa. Revista USP. São Paulo:116, 45-58.

Güera, D., Delp, E. J. (2018). Deepfake video detection using recurrent neural networks. In IEEE International Conference on Advanced Video and Signal-based Surveillance (to appear). Doi: 10.1109 / AVSS.2018.8639163

Hasan, H. R., Salah, K., (2019). Combating Deepfake Videos Using Blockchain and Smart Contracts. in IEEE Access. 7, 41596-41606. doi: 10.1109/ACCESS.2019.2905689.

Joseph, R. (2019). Fakebusters strike back: How to spot deep fakes, the manipulated videos that are the newest form of "fake news" to hit the internet. *Index on Censorship*, 48(1), 76–79. doi: https://doi.org/10.1177/0306422019841326

Koopman, M., Rodriguez, A. M., & Geradts, Z. (2018). Detection of Deepfake Video Manipulation.In: Conference: IMVIP, At Belfast. August 2018. Recuperado de https://www.researchgate.net/publication/329814168_Detection_of_Deepfake_Video_Manipulation

Korshunov, P., Marcel, S. (2018). DeepFakes: A new threat to face recognition? assessment and detection. arXiv:1812.08685v1 [cs.CV] 20 Dec 2018. Recuperado de http://publications.idiap.ch/downloads/reports/2018/Korshunov_Idiap-RR-18-2018.pdf

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature. 521,436-444. doi: 10.1038/nature14539.
Li, Y., Lyu, S. (2018). Exposing deepfake videos by detecting face warping artifacts. arXiv:1811.00656v1 [cs.CV]. Recuperado de https://arxiv.org/abs/1811.00656

Maras, M.-H., & Alexandrou, A. (2018). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. *The International Journal of Evidence & Proof*, 23(3), 255–262. doi: https://doi.org/10.1177/1365712718807226

Miyoung, C., & Youngsook, J. (2016) Face recognition performance comparison between fake faces and live faces. Soft Computing 21(12), 3429-3437. Recuperado de https://link.springer.com/content/pdf/10.1007%2Fs00500-015-2019-4.pdf

Ngiam, J., Khosla, A., Mingyu, K., Juhan, N., Honglak, L., Ng, A.Y. (2011). Multimodal Deep Learning. Proceedings of the 28th International Conference on Machine Learning, ICML 2011. 689-696. Recuperado de https://www.researchgate.net/publication/221345149_Multimodal_Deep_Learning

Popescu, A. C, Farid, H. (2005). Exposing digital forgeries by detecting traces of resampling. in *IEEE Transactions on Signal Processing.* 53(2),758-767. doi: 10.1109/TSP.2004.839932

Sabir, E., Cheng, J., Jaiswal, A., AbdAlmageed, W., Masi, I., and Natarajan, P. (2019). Recurrent convolutional strategies for face manipulation detection in videos. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 80-87. Recuperado de https://arxiv.org/abs/1905.00582

Sullivan, B. (2019). Charniak, E. An *Introduction to Deep Learning. Perception*, 48(8), 759–761. doi: https://doi.org/10.1177/0301006619857273

Tan, X., Li, Y., Liu, J., & Jiang, L. (2010). Face liveness detection from a single image with sparse low rank bilinear discriminative model, Computer Vision ECCV 2010. Springer, Berlin Heidelberg.

Xin, Y., Yuezun, L. & Siwei, L. (2018).Exposing Deep Fakes Using Inconsistent Head Poses. ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, United Kingdom, 2019. 8261-8265. doi: 10.1109/ICASSP.2019.8683164.

Notas al final

i Aplicativo que tem como principal função a possibilidade de modificar as suas fotos, mais precisamente os selfies, transformando seu rosto em uma versão completamente inusitada.

ii Tecnologia que estabelecer a identidade de um indivíduo com base em um ou mais características fisiológicas ou comportamentais, tais como rostos, impressões digitais, íris e até vozes.

iii Aplicativo desenvolvido para smartphones utiliza inteligência artificial para transformar a foto do usuário, com filtros que permitem simular alterações em sua aparência física.

iv Ferramenta que utiliza aprendizado profundo para reconhecer e trocar faces em fotos e vídeos com base no código original do deepfakes.

v É uma expressão bastante comum entre os usuários das redes sociais, na internet. Consiste de uma palavra-chave antecedida pelo símbolo #.

Dados dos autores

Cristiane Pantoja De Moraes
Possui graduação em Ciências Biológicas (Licenciatura Plena) pela Universidade Vale do Acaraú (2008); Possui experiência na área de zoologia e educação ambiental com ênfase em moluscos Achatina fulica Caracol Gigante Africano aplicados a projetos de políticas públicas em escola na área metropolitana de Belém, PA. Fui estagiária no laboratório de Ornitologia e Bioacústica da Universidade Federal do Pará. Tem experiência em morfofisiologia do sistema visual em (Dasyprocta aguti) pelo laboratório de neurobiologia da Universidade Federal do Pará. Atualmente é discente do curso de Bacharelado em Biblioteconomia pela Universidade Federal do Pará(UFPA). Discente cursos de pós-graduação lato sensu (especialização) a distância em Gestão de Documentos e Informação pela Faculdade Unyleya.
crikapj@gmail.com

Received: 2020-01-16
Accepted: 2020-11-29