Ministry of Science and Higher Education of the Republic of Kazakhstan
L.N. Gumilyov Eurasian National University

Faculty of Information Technology
Department of Information Systems

DEEPFAKE

Done by: Zhumabek A.R
Check: Zhukabaeva T.K

Deepfake technology literally translates as “fake with the help of deep learning”. With its help, the face in the original image or video is replaced by the face of another person, with the accompanying adjustment of appearance parameters. The technology is based on GAN-neural networks. One such network consists of two networks, which “compete” with each other, generating many images and coming to a “common solution”.

In very simple terms, a dipfake is the replacement of one face in a picture/video with another one specified by the user. This technology is used, among other things, to create gossip about media personalities, but much more often just for fun.
In addition to the entertainment industry, dipfakes are also used to make fake videos with famous people. They can be the same actors, politicians, entrepreneurs - anyone. The combination of AI technologies with CGI-technologies gives a truly amazing effect and vast possibilities, which can be used both for good and not the most legitimate purposes.

A BIT OF HISTORY

Video and audio synthesis technologies have been developed since the late 1990s. In 1997, the company Video Rewrite presented a technology that simulates facial articulation for a synthesized audio track.
For a long time these technologies remained in the narrow circle of specialists, but in 2009 Avatar demonstrated their wide possibilities.
In 2014, Audrey Hepburn “starred” in a commercial, and the 2019 film “The Irishman” used AI to rejuvenate actors.
Previously, synthesized video was created manually, but with the development of machine learning, dipfakes have become more realistic and work in real time.

THE EMERGENCE OF REAL DEEPFAKES

Deepfake's technology uses neural networks to synthesize images and soundtracks, learning from thousands of examples of faces and voices. This allows the AI to produce realistic results.
The name Deepfake emerged in 2017 when a Reddit user with the nickname Deepfake created some controversial celebrity videos. Since then, the term has stuck to such technologies.
Synthetic content generation companies have been active in recent years. YouTube channels Shamrock, Ctrl Shift Face and easy-to-use apps have made Deepfake a mass phenomenon. Virtual stars like Lil Michela have emerged in the entertainment industry.
As technology advances, dipfakes will become even more realistic and everyday. The question is who controls their development, where they are applied and what to expect in the future.

HOW DO DIPFAKES WORK?

Deepfakes are created using deep learning algorithms that analyze images and audio and then generate realistic fakes.
Core technologies:

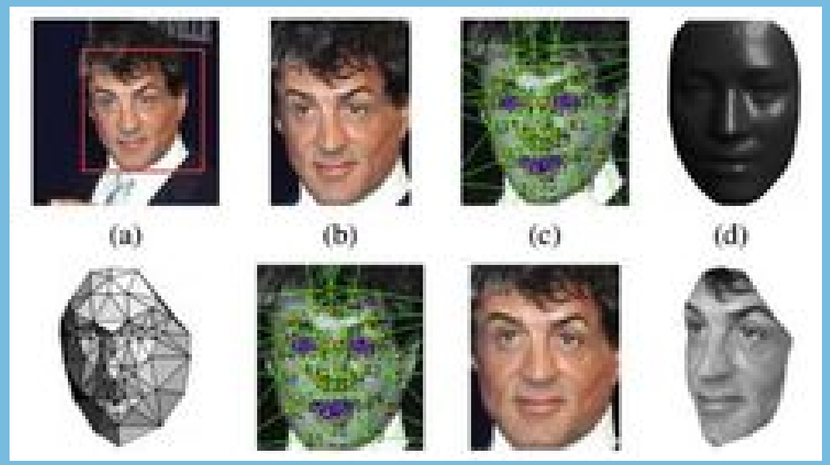
- Generative-adversarial networks (GANs) - consist of two neural networks:

A generator creates fake images or videos.
The discriminator tries to distinguish the fake from the real image.
During training, the networks improve and the dipfake becomes more and more realistic.

- Autoencoders (Autoencoders) are neural networks that compress and reconstruct images by learning their key features.
- NeRF (Neural Radiance Fields) - a new technology that can reconstruct 3D images from 2D photos.

The process of creating a dipfake

- Data collection - videos or photos of the person whose features will be used are uploaded.
- Model training - the neural network analyzes facial features, facial expressions and voice.
- Video or audio generation - the model synthesizes a fake, replacing the face or voice.
- Post-processing - artifacts are removed, lip movement and lighting synchronization are improved.



TOOLS FOR CREATING DIPFAKES

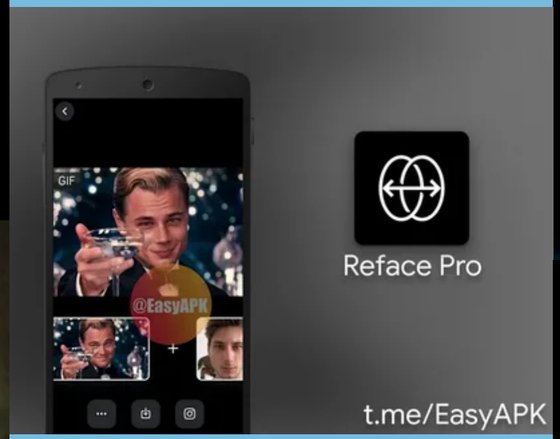
DeepFaceLab - professional tool for spoofing faces in videos.

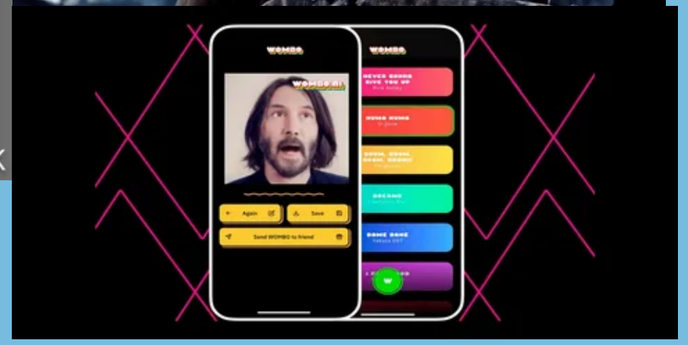
FaceSwap - open source software for creating dipfakes.

ZAO - mobile app that allows you to replace a face in a video in seconds.

Reface - entertainment app for real-time dipfakes.

Wombo AI - makes static images animated by making them “sing”.





WHERE ARE DIPFAKES USED?

Useful and legal applications

✅ Film and entertainment industry - rejuvenating actors, replacing faces (e.g., The Irishman, Star Wars).

✅ Education and science - recreating historical figures, assisting in learning.

✅ Gaming and virtual reality - realistic game characters.

✅ Medicine - dipfake technology helps patients with voice loss by creating synthetic speech.

Dangerous and illegal uses

❌ Disinformation and fake news - fake videos of politicians can influence public opinion.

❌ Fraud - dipfake voices are used to steal money (calls from “directors” to employees).

❌ Document forgery - use of dipfakes in biometric identification systems.

HOW TO RECOGNIZE DIPFAKE?

Visual signs of dipshake

🔍 Abnormalities in facial movement - flickering, abrupt or unnatural expressions.

🔍 Eyes and blinking - dipfeukes often have abnormal blinking frequency or unnatural reflections in their eyes.

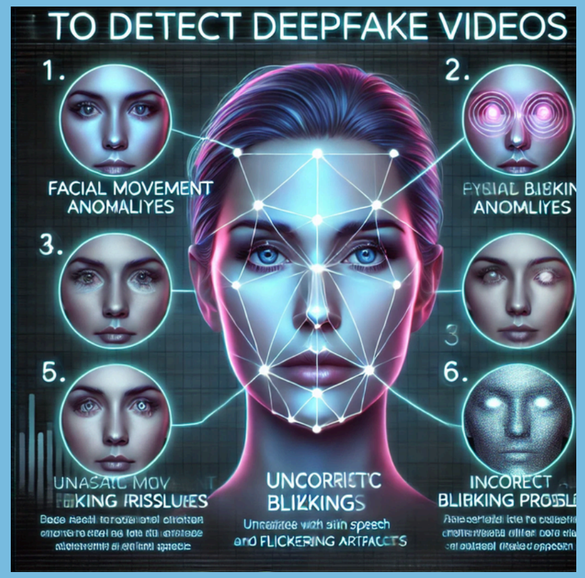
🔍 Unnatural skin - blurry or overly smooth areas, uneven lighting.

🔍 Mismatched shadows and lighting - shadows may not look right or may not move with the face.

🔍 Problems with teeth and lips - blurring, irregular contours, mismatched speech and lip movement.

🔍 Facial border anomalies - distortion or blurring around the edges, especially in the hairline area.

Whoever makes and distributes them. If a dipfake is used to deceive or harm, its author may be responsible. Social networks are also partly to blame if they don't remove fakes. And the people who send them out further may also be liable.



How can you protect your data from fakes?

🔹 Don't put a lot of photos and videos out in the open.

🔹 Set up privacy settings on social networks.

🔹 Add watermarks to your photos.

🔹 Check for suspicious videos.

🔹 Be careful with voice messages - a fake voice can be spoofed.

🔹 Keep an eye out for new security methods.

Deepfake Detection Tools

- Deepfake Detector - analyzes video for signs of fake.
- Microsoft Video Authenticator - detects changes in image pixels.
- FaceForensics++ - a set of tools for automatic detection of dipfakes.

CONCLUSION

Deepfakes are a powerful technology that can be both useful and dangerous. They are used in movies, games and marketing, but they can also mislead people, fake identities and spread false information.
It's important to be able to tell the difference between a dipfake and a real video, protect your data and be vigilant online. Technology continues to evolve, and with it should come evolving methods of protection. Ultimately, people are responsible for their use.

```python
import cv2
import dlib
import numpy as np
from google.colab.patches import cv2_imshow
import os

if not os.path.exists("/content/shape_predictor_68_face_landmarks.dat"):
    raise FileNotFoundError("Файл shape_predictor_68_face_landmarks.dat not found!")
detector = dlib.get_frontal_face_detector()
predictor = dlib.shape_predictor("/content/shape_predictor_68_face_landmarks.dat")

def get_face_landmarks(image):
    gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)
    faces = detector(gray)
    if len(faces) == 0:
        raise ValueError("Mistakes")
    landmarks = predictor(gray, faces[0])
    points = np.array([(landmarks.part(n).x, landmarks.part(n).y) for n in range(68)], dtype=np.int32)
    return points
def delaunay_triangulation(points, size):
    rect = (0, 0, size[1], size[0])
    subdiv = cv2.Subdiv2D(rect)
    for p in points:
        subdiv.insert(tuple(map(int, p)))
    triangles = subdiv.getTriangleList()
    triangles = np.array(triangles, dtype=np.int32)
    delaunay_indices = []
    for t in triangles:
        pts = []
        for i in range(0, 6, 2):
            pt = (t[i], t[i+1])
            idx = np.argmin(np.linalg.norm(points - pt, axis=1))
            pts.append(idx)
        delaunay_indices.append(pts)
    return np.array(delaunay_indices)
def swap_faces(source_img, target_img):
    source_points = get_face_landmarks(source_img)
    target_points = get_face_landmarks(target_img)
    triangles = delaunay_triangulation(target_points, target_img.shape)
    mask = np.zeros_like(target_img, dtype=np.uint8)
    hull = cv2.convexHull(target_points)
    cv2.fillConvexPoly(mask, hull, (255, 255, 255))
    warped_source = np.zeros_like(target_img)
    for tri in triangles:
        pts_source = np.float32([source_points[tri[0]], source_points[tri[1]], source_points[tri[2]]])
        pts_target = np.float32([target_points[tri[0]], target_points[tri[1]], target_points[tri[2]]])
        M = cv2.getAffineTransform(pts_source, pts_target)
        warped_triangle = cv2.warpAffine(source_img, M, (target_img.shape[1], target_img.shape[0]))
        mask_triangle = np.zeros_like(target_img, dtype=np.uint8)
        cv2.fillConvexPoly(mask_triangle, np.int32(pts_target), (255, 255, 255))
        warped_source = cv2.bitwise_and(warped_source, cv2.bitwise_not(mask_triangle))
        warped_source += cv2.bitwise_and(warped_triangle, mask_triangle)
    center = (target_points[:, 0].mean().astype(int), target_points[:, 1].mean().astype(int))
    seamless = cv2.seamlessClone(warped_source, target_img, mask, center, cv2.NORMAL_CLONE)
    return seamless

source_img = cv2.imread("/content/3.jpg")  # first face
target_img = cv2.imread("/content/7.jpg")  # second face

if source_img is None or target_img is None:
    raise ValueError("Mistake with import!")
result = swap_faces(source_img, target_img)
cv2_imshow(result)
cv2.imwrite("/content/swapped_face.jpg", result)
```

This code replaces a face in a photo using Delaunay triangulation and seamless cloning method. It first finds the key points of the face using dlib, then breaks the face into triangles and transfers them to the new image with affine transformations. At the end, we use cv2.seamlessClone to seamlessly embed the face, preserving lighting and texture. The end result is a realistic Deepfake effect

THANK YOU

References

- https://habr.com/ru/companies/neuronet/articles/592119/
- https://wotpack.ru/15-deepfake-nejrosetej-chtoby-sdelat-video-i-foto-v-2023-godu/
- https://blog.eldorado.ru/publications/chto-takoe-deepfake-10-luchshikh-prilozheniy-dlya-sozdaniya-dipfeykov-35408
- https://medium.com/nerd-for-tech/deep-face-recognition-in-python-41522fb47028