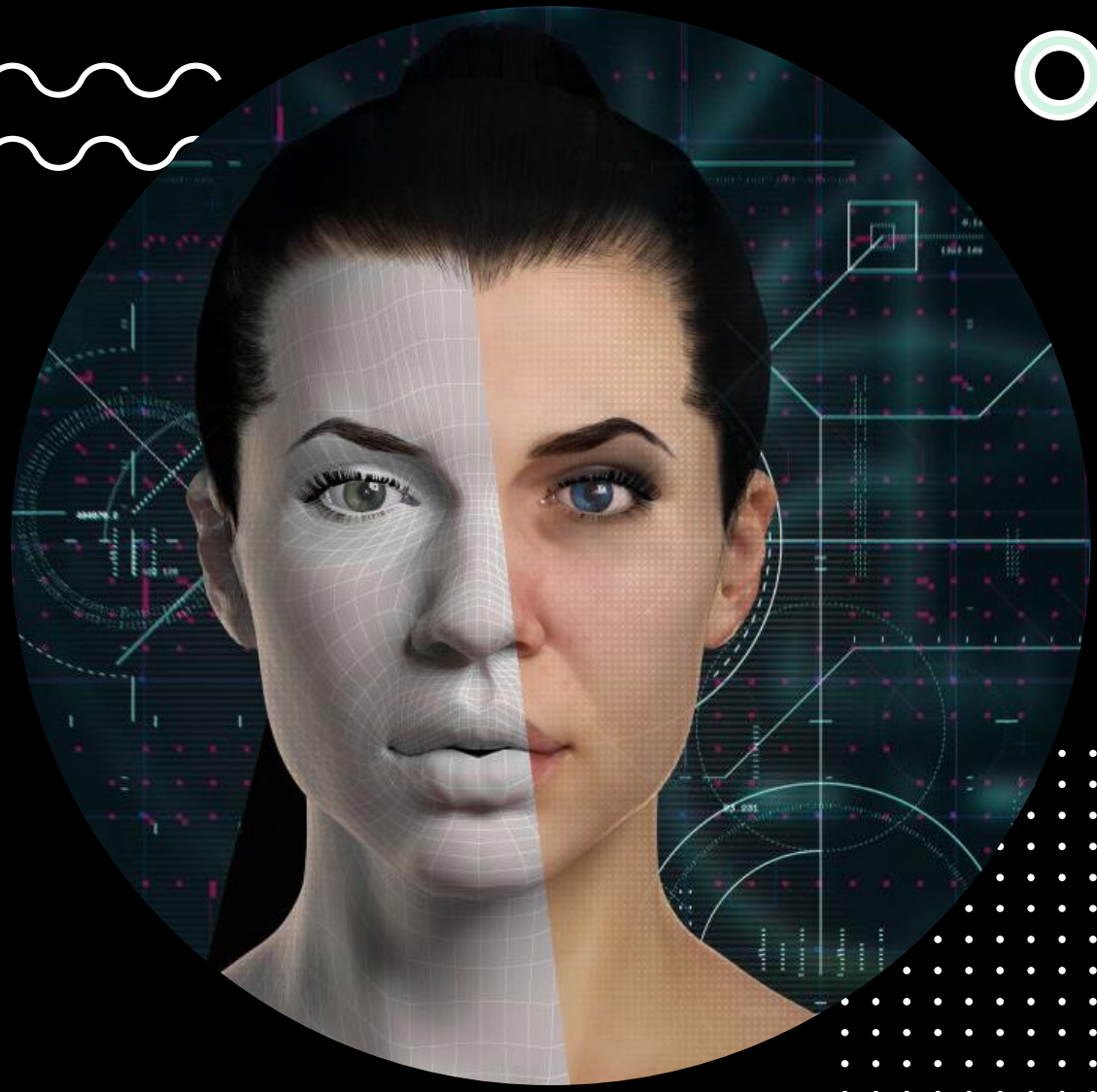
# EMERGENCE OF DEEPFAKE TECHNOLOGY



Aththanayaka P.A.G.P.B.

# Content

- Abstract
- Introduction
- Evolution of Deepfake Technology
- Future of Deepfake Technology
- Conclusion

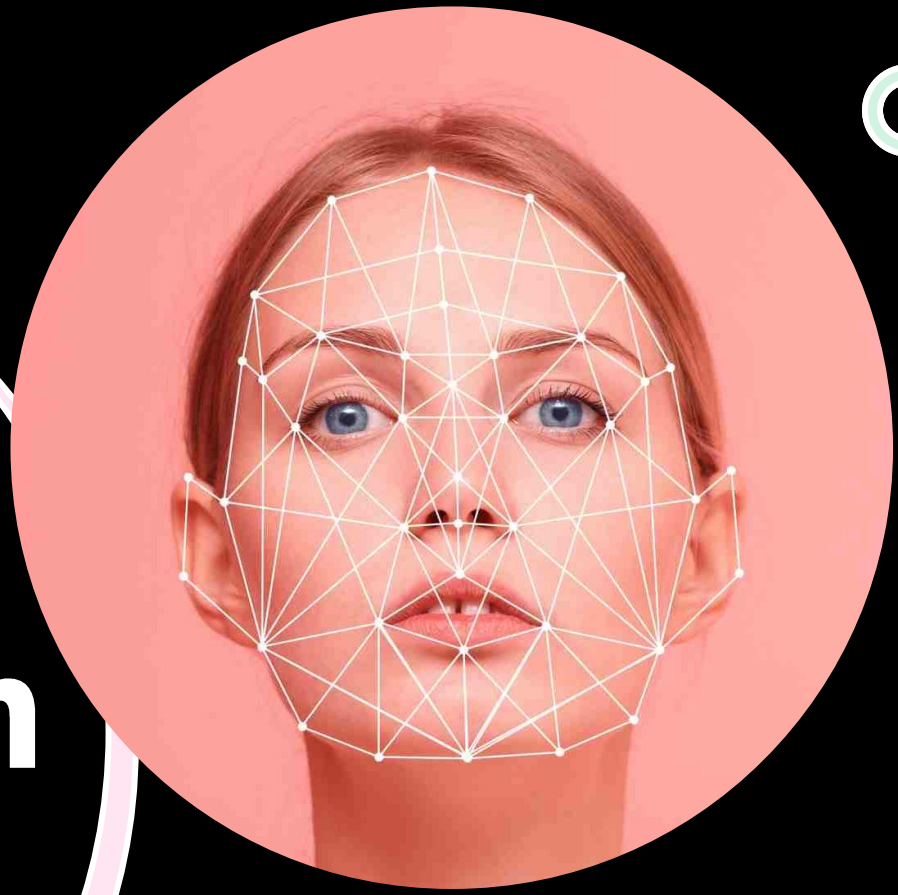
# Abstract

The present-day digital technologies make it hard for the human brain capacity to detect what are the real technologies and what are fake. Deepfake technology is one of the most recently developed and emerging technology which marked a turning point in the creation of fake content.

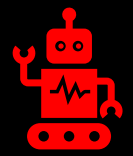
In this presentation, there will be explained content such as what is deepfake, which kind of parties generate deepfakes, what are the beneficiaries and negative impacts of deepfake technology, Examples of deepfakes, countermeasures against deepfake and the future development of deepfake technology.

# Introduction

*Introduction to deepfake technology*

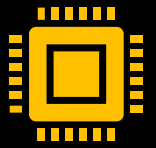


# Introduction to Deepfake Technology



Deepfake is an Artificial intelligence and machine learning based technology made by highly enthusiastic techniques that can basically replace a face with another.

The main purpose of this technology is, to swap the face of a targeted person to a video acted by someone else. That acting person preventing like the targeted person and he or she is saying and doing things the targeted person does.



Some deepfake content can be created using computer graphics and visual and some deepfake content can be created using sophisticated models such as auto encoders and generative adversarial network.

Deepfake Technology holds both advantages and disadvantages.

# Evolution

*Evolution of the domain of deepfake technology*

# Evolution

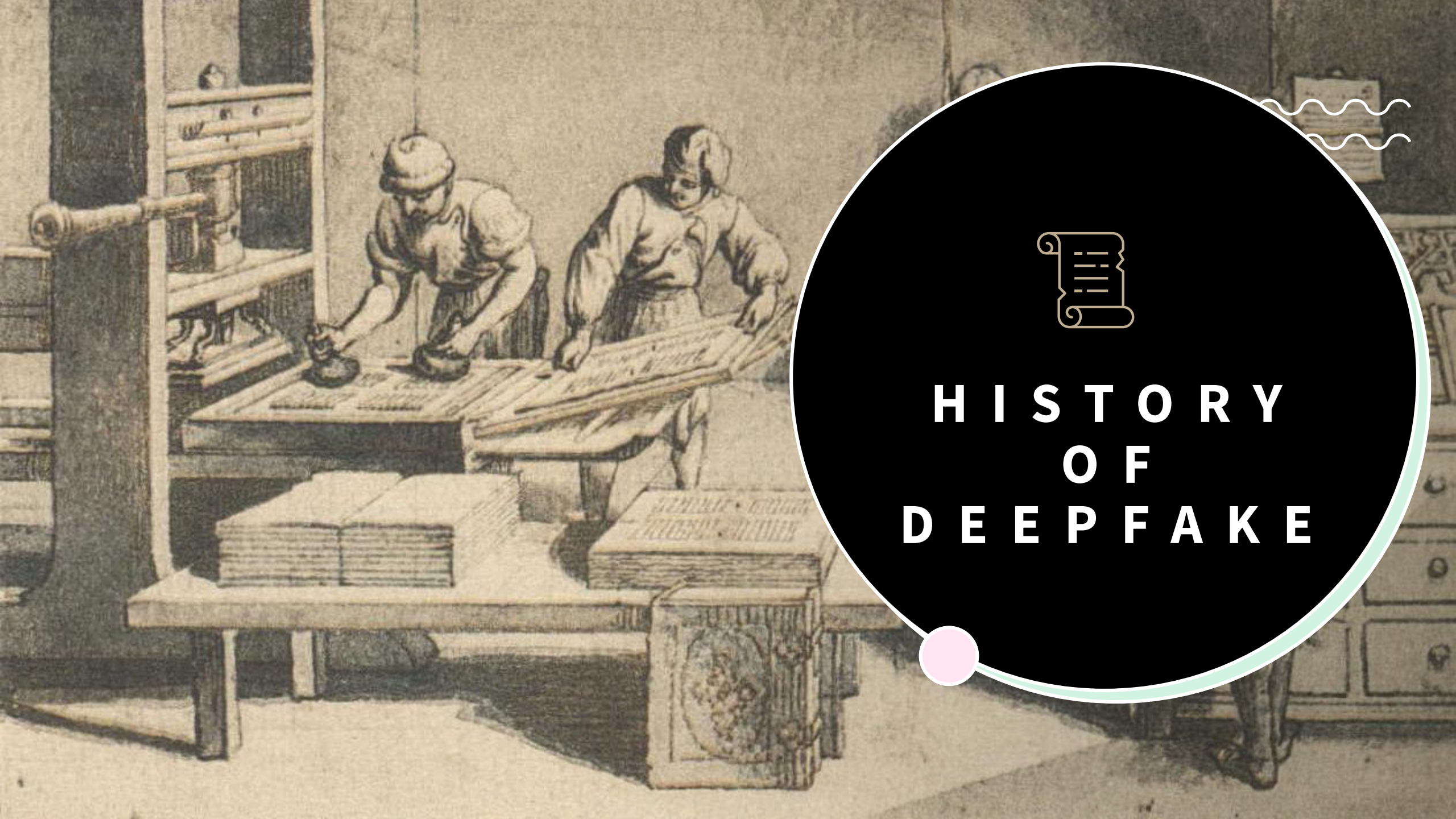
History of Deepfake technology

Uses of Deepfake

Deepfake creation process

Responses taken against Deepfakes

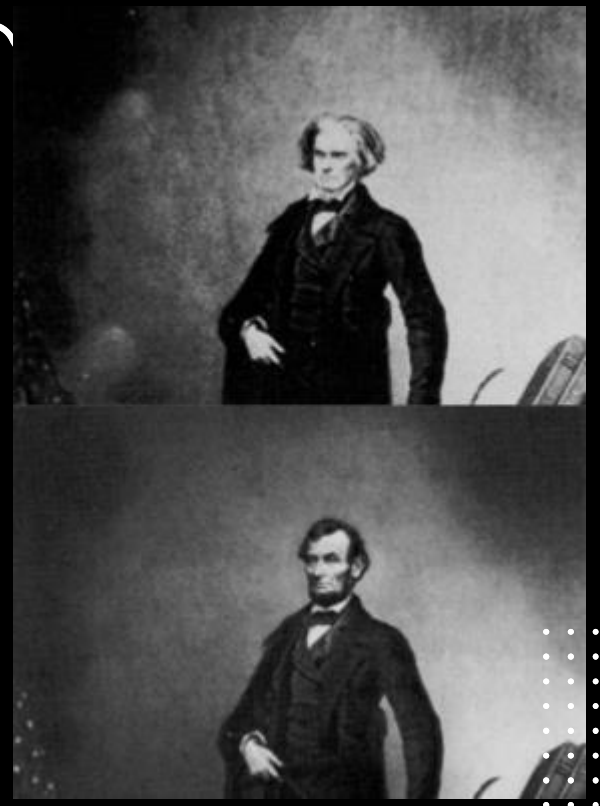
Deepfake detection process

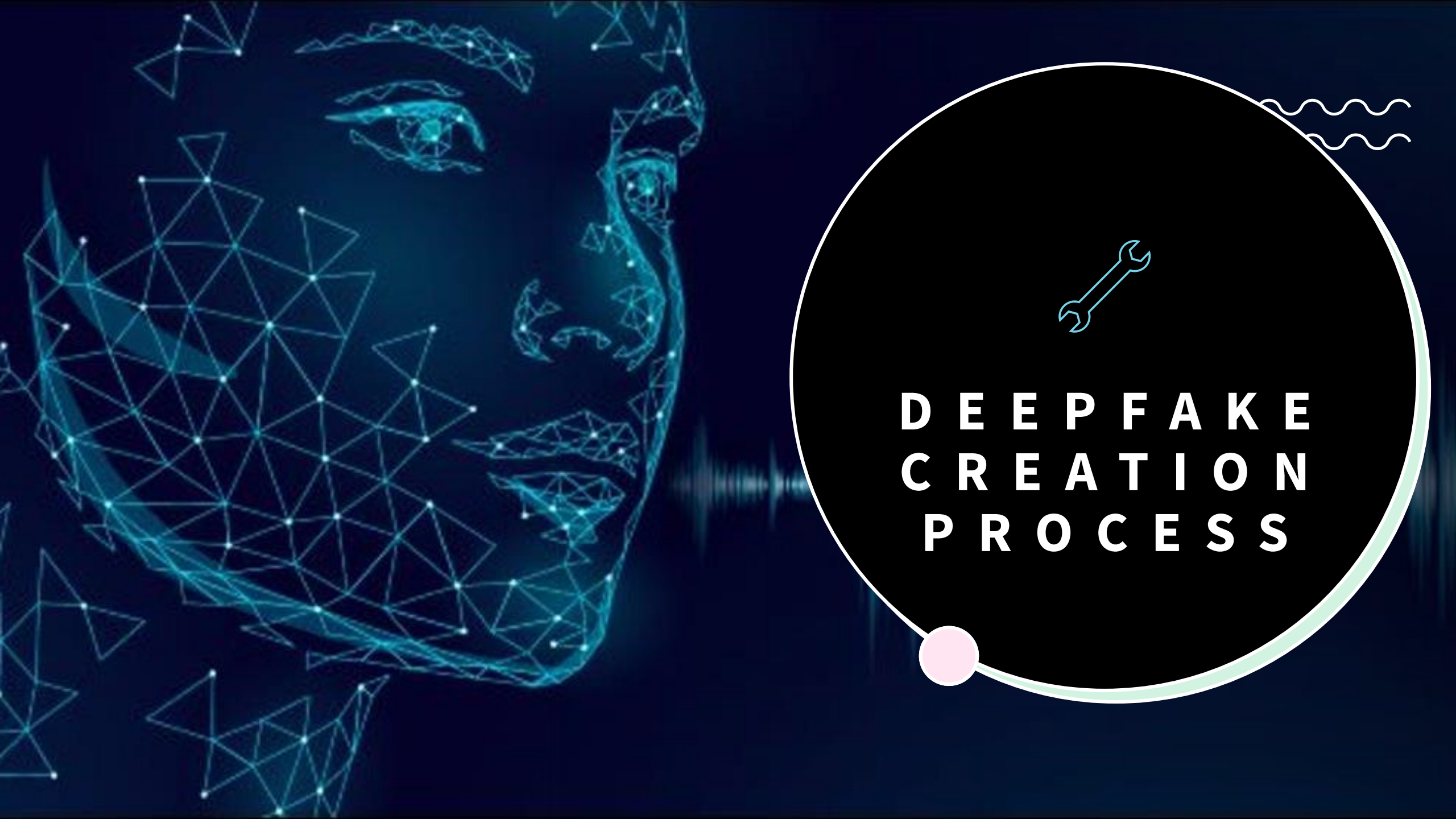


# HISTORY OF DEEPFAKE

# History of Deepfake Technology

- Idea of a deepfake content was firstly raised around 1865.
- It was the first known attempt to change the face of someone with another face using a painting.
- Former US president, Abraham Lincoln's face was swapped with the body of John Calhoun who was a politician in the southern US.
- Demand for that deepfake painting was surprisingly increased after Abraham Lincoln's death.

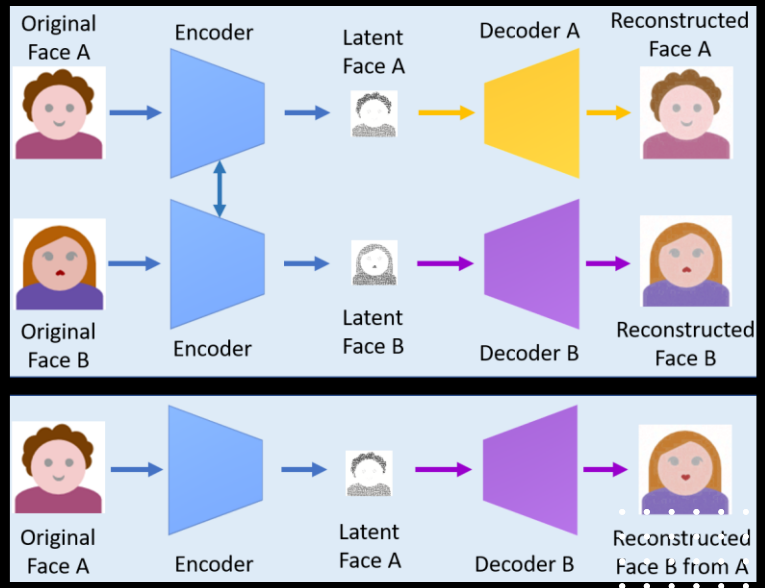




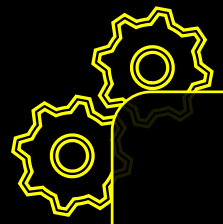
# DEEPFAKE CREATION PROCESS

# Deepfake creation process

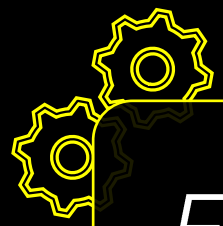
- Deepfakes have emerged as famous since the superiority of content and additionally, the convenience of use of the applications to a huge range of users with diverse technical skills from expert to apprentice.
- The first strive of creating deepfake creating module was *Faceswap* which developed utilizing the technology called autoencoder-decoder pairing structure
- By combining adversarial loss and perceptual loss techniques to the autoencoder-decoder architecture, an improved version based on the generative adversarial network known as GAN was developed.
- After the invention of the major idea, number of deepfake creation tools were discovered.



# Deepfake tools



*Faceswap*



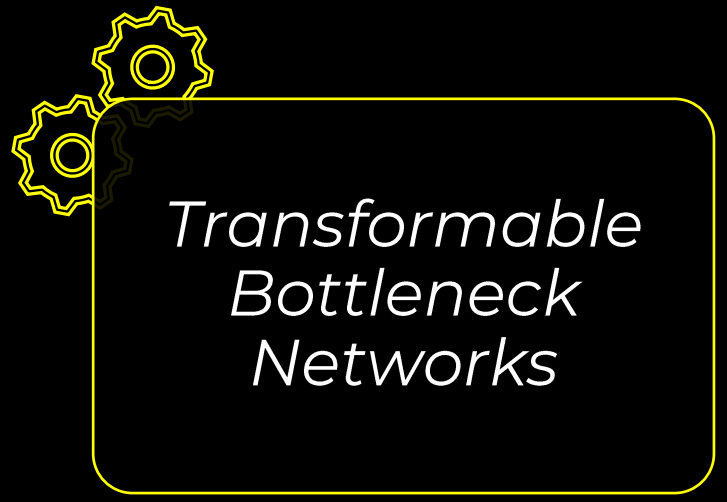
*Faceswap GAN*

*Few-Shot Face Translation*

# Deepfake tools

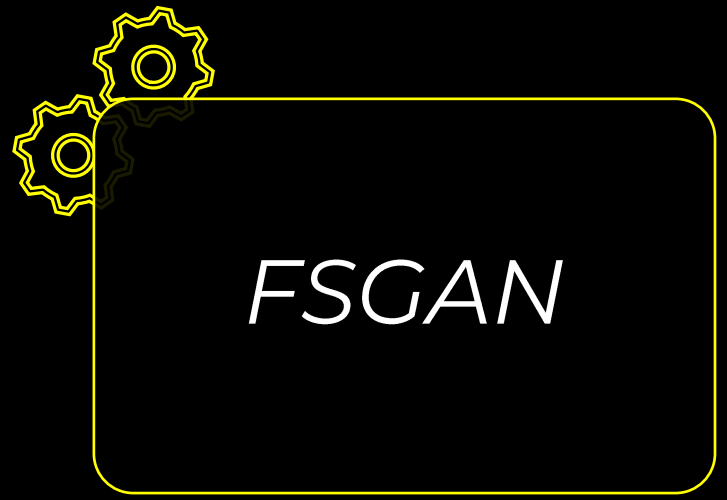


# Deepfake tools

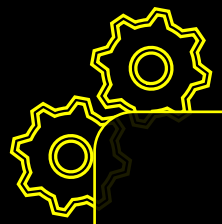




# Deepfake tools

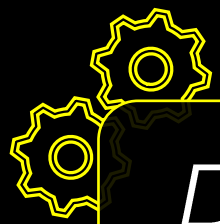




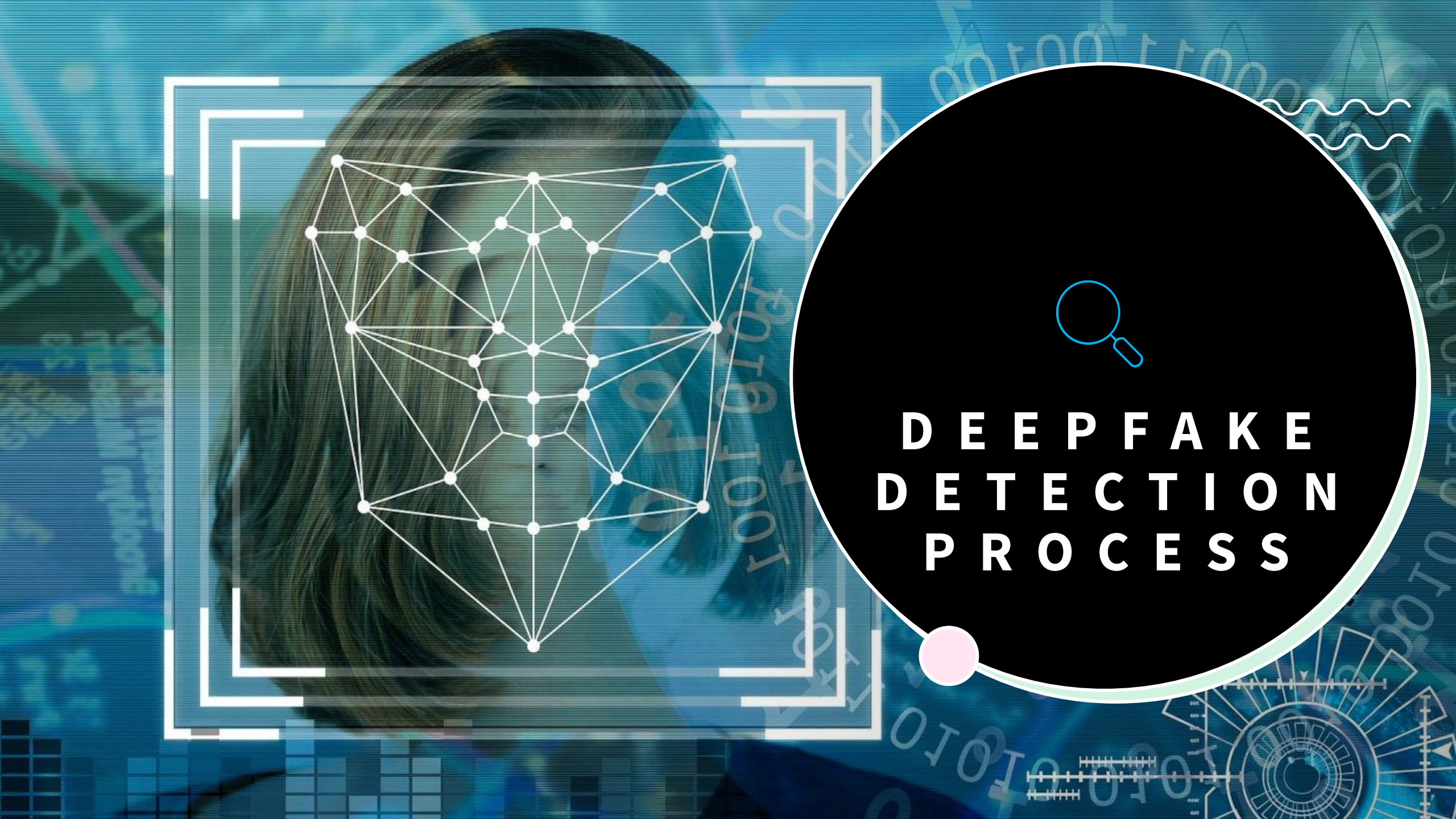
# Deepfake tools



*Neural Voice Puppetry*

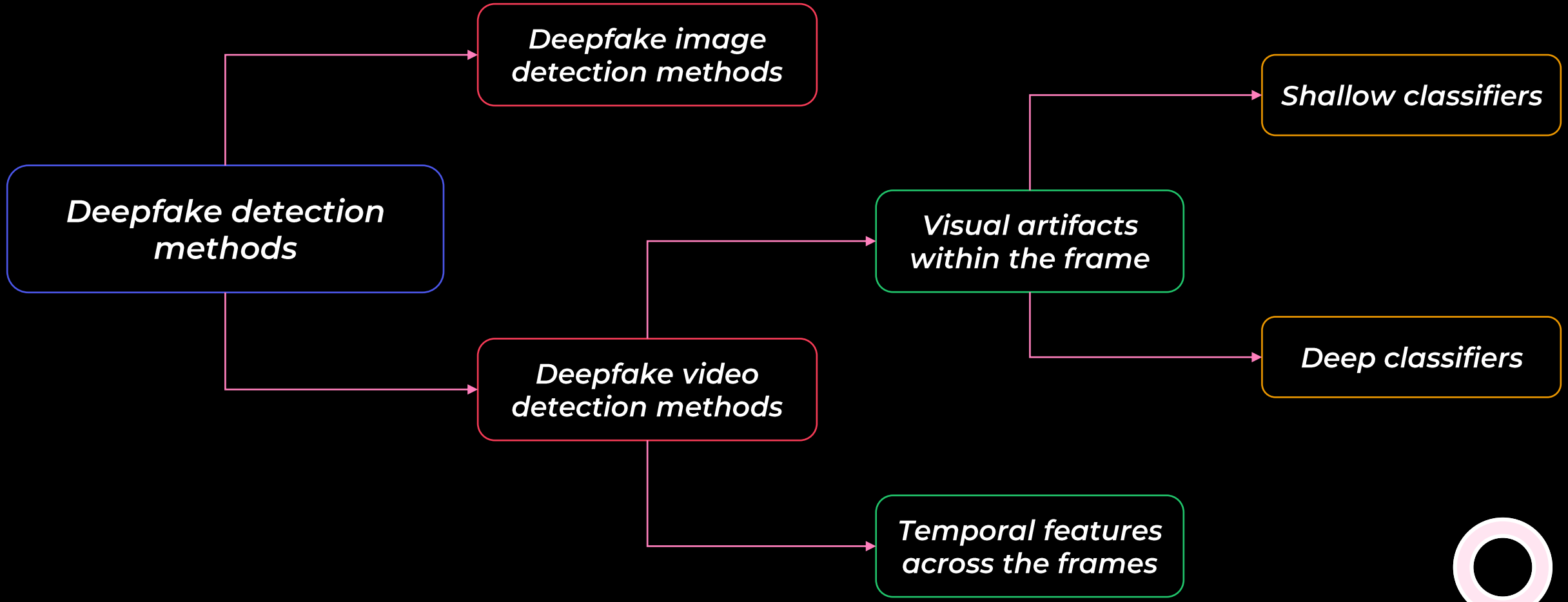


*Do as I Do Motion Transfer*


DEEPFAKE
DETECTION
PROCESS

# Deepfake detection process

- The classical method to detect deepfake images and videos was a natural approach that examines manually and finds inconsistencies and artifacts of the fake content creation process
- The Modern approach is to find deepfake content is an automatic process. It can detect major and discriminative features of deepfake contents.
- Usually, deepfake detection tools using a binary classification system to examine and classify real content and fake content. This kind of strategy requires a database containing a huge number of real and fake videos to program the classification module.


Deepfake detection methods
Deepfake image detection methods
Deepfake video detection methods
Visual artifacts within the frame
Temporal features across the frames
Shallow classifiers
Deep classifiers

# Deepfake image detection methods

- Deepfake images are one of the most popular methods used by cyber attackers to exploit identification or authentication and gain access to unauthorized systems.
- Zhang and team were able to develop a method to detect deepfake images using bag of words strategy.
- Xuan and his team found image preprocessing method to detect fake images.
- Hsu and team proposed a two-phase deepfake detecting method.

# Deepfake video detection methods

- Most of the image detection methods and tools cannot be utilized for deepfake video detection.
- Reason for that is properties of a video sequence are changing rapidly from frame to frame.
- Deepfake video detection can divided into two parts named temporal feature across the frames and artifacts within the frame.

# Temporal features across the frames method

This methods detect deepfake videos by examine the overall properties of a video, across the frames.

Ekraam Sabir explains spatio temporal feature of video can be used to detect the deepfake videos. Based on that theory, the Recurrent convolutional model which known as RCN was developed.

David and Edward introduced that deepfake videos can be found using intra-frame inconsistence of videos.

Eye blinking is also a temporal feature of a video. Less frequency of eye blinking is also a property of a deepfake videos.

# Visual artifacts within the frame method

This method decompress video into frames in order to find visual artifacts in every frame.

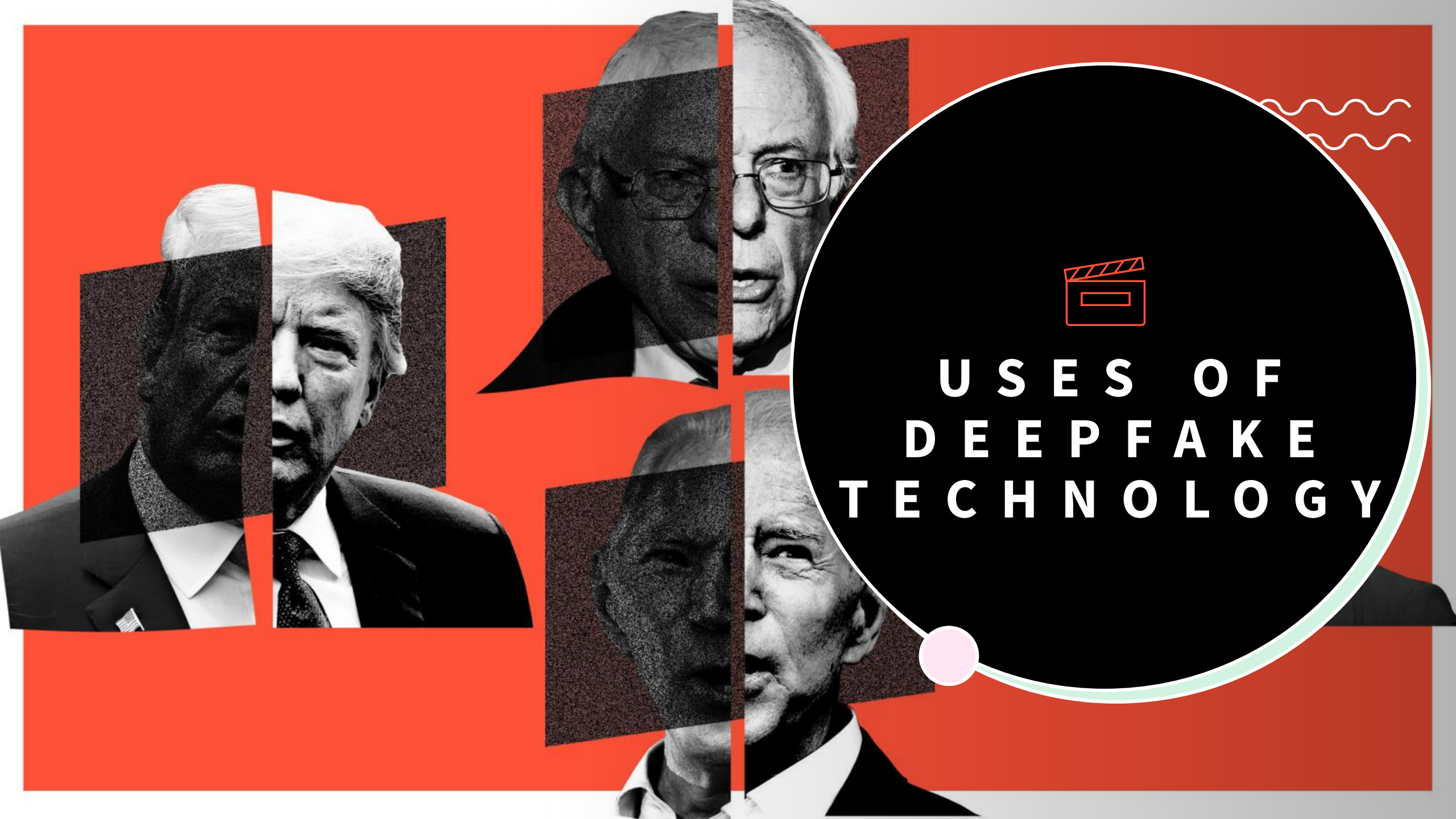
This approach divided into 2 parts named deep classifiers and shallow classifiers.

### Deep classifiers

Deep classifiers are used to find deepfake videos by the weaknesses that deepfake generating tools made when scaling and rotating the original image to fit into the fake videos

### Shallow classifiers

Shallow classifiers are used to find differences in pose and lightning in 3d face models using 68 of face landmarks.


USES OF
DEEPFAKE
TECHNOLOGY

# Blackmail

- Blackmail is requesting some advantage from someone as a trade-off for not revealing sensitive information about them.
- Using deepfake content as blackmailing material can be effective since the realities of the deepfake videos and images.
- Since the fake content cannot be reliably distinguished from real content, a victim who blackmailed can state that the even real content is fake. This is a major issue for the real blackmailers which is known as blackmail inflation.

# Politics

- Politics is the most targeted domain of the deepfake creators. What deepfake content can do is simply mispresent a politician in a video or in an image.
- In 2018, A popular American actor, comedian, and filmmaker Jordan Peele made a deepfake video associated with an entertainment company named BuzzFeed.
- In 2019, an employee who worked at the KCPQ channel which owned by the Fox television network made a deepfake video targeting Donald Trump
- In 2020, a deepfake video was published that made targeting Belgian Prime Minister Sophie Wilmes. That video was about a connection between Covid-19 and deforestation

# Movie Industry

- Utilizing deepfakes in the Digital entertainment industry can consider as a positive impact of deepfake technology.
- Using deepfake technology producers can create a younger version of an actor for the prequel movies that have been become very popular recently.
- The world-famous movie-making company: Disney is a leading company among the companies that use deepfake technologies in their movies. They developed a model with the capability to identify facial expressions and face-swapping which generate high-quality outputs with 1024x1024 resolutions.

# RESPONSES TAKEN AGAINST DEEPFAKE

# Responses against Deepfake

- In 2018, the Deepfake content prohibition act was acquainted with the US Senate.
- In 2019, Act against the Deepfake liability was introduced for the first time at the house of Representatives.
- In several states in the US like New York, Virginia, and Texas, there are different kinds of rules against the deepfakes.
- Huge social media networks such as Facebook and twitter are also taking responses against deepfake networks.

# Future of Deepfake

*Future developments of deepfake technology*

# Future of Deepfake

- Deepfake will be a general topic.
- Advantages of deepfake will increase as well as the disadvantages.
- Number of Cyber crimes will increase.
- Using new technologies, deepfake technology will be more realistic and undetectable.

# Conclusion

As described under that topics, it is clear that deepfake technology is not a domain that will end up being built. The continuous evolvement of the deepfake content creating methods as well as deepfake detecting methods is the main reason for that.

If there is a chance to enhance more in the deepfake detection domain and if deepfake technology can be adapted in a more advantageous way, there is no doubt that there will be a revolution in digital media technology in the future.

# THANK YOU