

heating the oven before you arrive, adjusting blinds as sunlight shifts, or dimming lights when fatigue patterns emerge – creating proactive living that enhances comfort while reducing energy waste [6].

These capabilities converge to elevate security, efficiency, and well-being: the house detects anomalies with contextual awareness: distinguishing a family member from an intruder, optimizing weather forecasts, automates multi-device orchestration seamlessly, and evolves over time as it integrates more data streams. The result is an environment that actively strives to improve daily life, moving beyond convenience to a responsive partner that learns your rhythms and adapts without constant input. Real-world implementations already demonstrate this trajectory, proving AI's power to make homes not just smarter, but truly alive with foresight and empathy [6].

For conclusion, AI transforms a smart house from a rigid, rule-based system into a proactive, adaptive environment that learns user habits, optimizes energy use, enhances security, and simplifies daily life through natural interaction. Despite challenges such as high costs, privacy risks, and complexity, AI-driven homes are becoming the new standard of modern living – delivering personalized comfort, predictive maintenance, and sustainable efficiency.

References

1. Smart Home: Definition, How It Works, Pros and Cons; (<https://www.investopedia.com/terms/s/smart-home.asp>)
2. The Smart Home Never Quite Worked. Now It's Getting an A.I. Reboot. (<https://www.nytimes.com/2026/03/05/technology/personaltech/ai-smart-home-google-gemini-amazon-alexa.html>)
3. How to Integrate AI Into Smart Home Application for Smarter Living (<https://labs.lamatic.ai/p/how-to-integrate-ai-into-smart-home-application/>)
4. The Intelligent Abode: How Artificial Intelligence is Redefining the Smart Home; (<https://medium.com/@ajayverma23/the-intelligent-abode-how-artificial-intelligence-is-redefining-the-smart-home-18c6aa993f38>)
5. What Are the Pros of Having a Smart Home? And Are There Any Cons? (<https://therecursive.com/what-are-the-pros-of-having-a-smart-home-and-are-there-any-cons/>)
6. The future of Smart House (<https://webmobtech.com/blog/ai-for-smart-homes-revolution/>)

EVOLUTION OF DEEPAKES: FROM AN INTERNET JOKE TO A PERFECT ILLUSION

*Shypunova A. V., student,
Poliakova T. L., Associate Professor
National Technical University “Kharkiv Polytechnic Institute”.*

Artificial intelligence nowadays is a frequently discussed topic. It is widely discussed in the media and everyday life – on the radio, on the news, from your friends or colleagues at work. It completely deserves the significant attention it gets.

To acknowledge the full size of the evolution of AI, let us look back into 2023. On March 23, a user of the platform “Reddit” under the nickname StableDiffusion posted an AI-generated video. The video was created using the ModelScope text-to-video tool and featured a distorted, surreal version of the famous American actor Will Smith who was eating spaghetti. During the video his face was “moving chaotically and movements looked unnatural”. Because of that, some users even called the video “eerie” and “demonic”. That moment was, probably, the beginning of the active and fast evolution of AI as a content-maker, which now turned into something powerful and unlikely to stop developing.

This amusing prompt became a standard for evaluating the realism and coherence of AI-generated videos, widely known as "The Spaghetti Benchmark." As large language (such as ChatGPT, Gemini, Claude) and multimodal (Sora, Veo) models continue to evolve, developers use this test to identify improvements. And they don't keep us waiting. In May 2024, Veo, an AI-based tool powered by Google, presented the enhanced version of the video with the same prompt – “Will Smith eating spaghetti”. It demonstrated significant improvements in facial accuracy, fluid motion, and audio synchronization.

People who have access to the internet have seen an AI-generated video at least once in their life, but this number is likely to be much higher. Usually we can recognize it easily – the plot is often obviously unreal and comic, as for instance cats walking on two legs like humans and falling in love with each other and all of that is accompanied by a dramatic melody. That is clearly a product of AI. Nobody would be even surprised by such kind of videos. However, how often does it happen that you watch an interesting video, then open the comments and find there something like “unfortunately it's AI”? Right after, an unpleasant feeling as if you were fooled appears. Exactly at that point –

where the obvious joke ends and visual fraud starts – the main problem of modern technologies is born. Video generation models have become the foundation for creating "deepfakes" – a technique that creates highly realistic fake images, audio, and video that allows for the convincing replacement of real people's faces and voices. What began as a funny internet trend is now breaking the borders between truth and fiction. Video footage is no longer undeniable proof of reality.

The purpose of this work is to track the evolution of deepfake creation, to analyze how they turned from the entertaining tool into a real cyber threat and what can be done to protect oneself from them.

A rapid switch from the obviously fake videos to the "ideal illusion" became possible thanks to the great step in machine learning algorithms. While the very first deepfakes were created on base of the simple generative networks, which were likely to make a lot of mistakes in textures and symmetry, a new generation of multimodal models are "educated" by the enormous amount of data. They take into account all details, starting with light reflection in the pupils and ending with eyebrows hairs.

One of the biggest victories of the AI-developers was overcoming the "Uncanny Valley effect". This is a psychological phenomenon, in which a human-like figure that looks and behaves almost like a real human, but has subtle differences, evokes feelings of discomfort and fear in observers. This is exactly what we experienced in 2023 with the Will Smith video. However, modern models have learned to imitate natural blinking, movements of the neck muscles during speech and even some defects of the skin. It takes away all the possible clues from our brain that allow recognizing a fake easily.

Another important part of the evolution of the deepfakes is their accessibility. Anyone with a smartphone can create his or her own deepfake video with any scenario. Just a few years ago, creating a high-quality face swap required powerful equipment, advanced programming skills, and weeks of creation. Today, this technology has been simplified – any smartphone user can download an app that can create a video in seconds. This simplicity of use has crossed the line between professional video production and common user-generated content.

The reason we fall for these traps is that our weakness in front of the deepfakes is conditioned not only by the growth of AI but also peculiarities of our own psychology. Evolutionarily, we are used to trusting what we see. Moreover, deepfakes creators often use "emotional hooks" – content is crafted to provoke an immediate reaction: anger, fear, joy or delight. In moments of intense emotional outburst, critical thinking is dulled, and we stop checking video details accurately, accepting what we see as truth. That is how technological progress took away our ability to distinguish truth from a lie with our eyes. In this way, deepfakes have evolved from modern experiments to a tool capable of manipulating reality. And this very “ideal illusion” is becoming the foundation for new, much more dangerous threats.

When the clear border between truth and fake was gone, a wide door full of opportunities was opened for criminals. And they took that opportunity without hesitation. As soon as the technology for generating realistic content became accessible, it quickly migrated from the arsenal of internet jokers to the tools of professional hackers and scammers. On a global level, deepfakes are used for major financial crimes, such as, for example, imitating a CEO's voice to steal millions, or creating fake political remarks to manipulate elections. There is a great variety of such cases. Nevertheless, all of that is far away from ordinary people. At the same time, when it comes to large companies that have money to purchase powerful security programs, common people remain unprotected. And here, the most important, and perhaps the most painful, target for AI fraudsters is the older adults. Older people grew up and lived most of their lives in a world where audio and video were absolute, non-negotiable proof of reality. If a relative called on the phone, it was really them. If someone appeared on television, it was not questioned. In contrast, younger generations are more familiar with the online environment and are intuitively expecting the digital world to be tricky. Older people often lack this so-called “digital skepticism” and may trust what they see on the screen without hesitation.

“With just a few seconds of audio taken from an Instagram Live video, a TikTok post, or even a voice note, fraudsters can create a believable clone that can be manipulated to suit their needs”, states the recent cybersecurity report by McAfee

(2023). The scheme is simple and verified – victims receive a call from their children or grandchildren. The voice of a relative usually sounds frightened or worried, telling about some imaginary tragedy – a car crash, a problem with the police, a sudden operation or something similar – and begging to send money as soon as possible. That is the moment, when that mechanism works like clockwork – a strong emotional shock and fear for a loved one turn off critical thinking. Older people cannot distinguish the slight metallic sound in a voice or unnatural pauses. A perfect illusion, mixed with parental instinct, makes such attacks almost flawless. Technological evolution has transformed deepfakes into a dangerous tool that is far from “friendly” to humanity.

This is how the digital “arms race” started – hackers and scammers are inventing more and more creative ways to get benefit from others’ losses while cybersecurity experts and law enforcement strive to develop protection against it. Just as the vaccine must be found when a new unknown disease captures the whole world, technological “antidotes” are now urgently required to stop the uncontrollable spread of deepfakes. The difficulty of this war lies in the fact that the virus is constantly mutating, just like its real biological prototype. As soon as security developers discover a breach in the generated videos, for example, unnatural blinking or a lack of facial expressions, deepfake creators immediately steal this data to train their own models. This creates a paradox: something that initially was meant to fight deepfakes is becoming fuel for them and a perfect material for development. This technological battle proves that correct algorithms alone are not enough to stand against this “sickness”. The real “vaccine” lies inside each of us – critical thinking, attention, and skeptical attitude to everything we can see online.

References:

1. McAfee. – Beware the Artificial Impostor: A McAfee Cybersecurity Artificial Intelligence Report. – 2023. – p. 7.
2. Uncanny valley. – Wikipedia. – 2024. – Available at: https://en.wikipedia.org/wiki/Uncanny_valley
3. Will Smith eating spaghetti. – Reddit (r/StableDiffusion). – 2023. – Available at: https://www.reddit.com/r/StableDiffusion/comments/1244h2c/will_smith_eating_spaghetti/
4. Will Smith Eating Spaghetti test. – Wikipedia. – 2026. – Available at: https://en.wikipedia.org/wiki/Will_Smith_Eating_Spaghetti_test