

The Role of Artificial Intelligence and Deepfake Applications in the Production and Dissemination of Electronic Rumors

Dr. Djemaa Mohammed

University of Bouira Mohamed.Djemaa@Univ-Bouira.Dz

Dr. Tarafi Sadek

University of Bouira s.tarafi@univ-bouira.dz

Abstract:

This study aims to illuminate one of the most significant and rapidly proliferating technologies in the contemporary digital landscape, particularly within the domains of content creation and digital media — namely, deepfake technology. As a branch of artificial intelligence, deepfake has evolved into a powerful and alarming tool for generating and manipulating content, enabling the production of images and videos of such high fidelity that distinguishing them from authentic material has become exceedingly difficult. The paper explores deepfake technology from a digital perspective, examining the key techniques and applications used in the fabrication and spread of electronic rumors, while presenting illustrative examples that convey both the significance of this technology and the severity of its threat across digital media platforms.

Keywords: Artificial Intelligence — Electronic Rumors — Deepfake

1. Conceptual Framework

1.1 Artificial Intelligence

Artificial intelligence (AI) is a branch of computer science concerned with developing machines capable of performing operations that simulate human cognitive processes, such as reasoning, learning, and error correction. More precisely, it is a field that seeks to understand and apply technology based on the computational emulation of human intellectual capacities (Abd al-Hadi, 2020, p. 20).

1.2 Falsification

Falsification is a material act and a form of deception through which an individual deliberately distorts the truth in a manner that inflicts harm upon the rights and legal standing of others (Khaddour, 2023, p. 5).

1.3 Deepfake

Deepfake refers to the technology that enables the creation of fabricated video content depicting individuals in scenarios that are, in many cases, virtually indistinguishable from authentic recordings (Al-Sharif, 2022, p. 327).

1.4 Algorithms

¹ Received: 15/01/2026; Accepted: 20/05/2026; Published: 07/10/2026

© 2026 The Author. Published by AVADA-CROMA. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, adaptation, and reproduction in any medium, provided that the original author and source are properly credited.
<https://creativecommons.org/licenses/by/4.0/>

Algorithms are logically ordered sets of procedures executed to achieve a specified objective or output. The term is commonly used as shorthand for programming instructions — those written and compiled by developers to produce an executable unit, also known as a program. Artificial intelligence systems are fundamentally dependent on algorithms and cannot function without them (Habib, 2019, pp. 98–99).

1.5 The Electronic Rumor

The electronic rumor — or digital rumor — represents a new strain of the networked information pathologies, a double-edged currency with two inseparable faces. Just as it can serve as a rallying point for mobilizing communities and promoting ideas, it is equally a destructive weapon for sowing panic, generating anxiety, and fueling aggression among individuals, groups, and even states.

The most widely cited definition of rumor is attributed to American sociologist Tamotsu Shibutani, who characterized rumors as improvised news generated through collective discussion. Shibutani argued that rumors originate from significant yet ambiguous events, and that the rumor constitutes simultaneously a channel for disseminating information and a channel for interpreting and commenting upon it. It is evident that Shibutani viewed the rumor as a collective act aimed at making sense of facts that lack adequate explanation (Jawad, 2024, p. 637).

Psychologist Arthur Reber, in his Dictionary of Psychology, defined rumors as "vague, inaccurate, or unverified reports or stories that circulate among members of a community, typically through word of mouth. Rumors tend to proliferate during times of social crisis and revolve around persons or events of public significance, particularly when information about those persons or events is unclear or incomplete" (Jawad, 2024, p. 638).

2. Advantages and Disadvantages of Artificial Intelligence

2.1 Advantages

1. *Fostering Creativity and Innovation*

Artificial intelligence is not merely a tool for streamlining routine tasks; it can serve as a catalyst for creativity across domains such as the arts, design, and musical composition. Algorithms are now being used to generate original paintings, architectural designs, and even film scripts.

2. *Supporting Economic Growth and Business Development*

AI enables startups to enhance their performance through precise market analytics, efficient resource management, and the development of personalized customer services based on behavioral and preference data. It also contributes to supply chain optimization and the reduction of operational waste.

3. *Mitigating Environmental Disasters and Climate Change*

AI systems are deployed in forecasting natural disasters — such as earthquakes and hurricanes — enabling the implementation of precautionary measures to minimize human and material losses. They are also used to optimize energy consumption and advance the development of clean energy sources, including solar and wind power.

4. *Developing Smart Systems in Cities and Communities*

AI contributes to the construction of smart cities that enhance quality of life by improving transportation networks, reducing urban congestion, rationalizing resource consumption, and bolstering public safety through intelligent surveillance and real-time emergency response systems.

5. *Enhancing Education Quality and Supporting Scientific Research*

Through adaptive learning, AI can design individualized curricula tailored to each student's level, enabling a more efficient educational experience. It also contributes to the development of smart classrooms that leverage virtual reality and AI to deliver interactive educational content. Furthermore,

AI technologies such as ChatGPT facilitate the rapid generation of textual content, saving researchers significant time and effort (Siham, 2024, p. 111).

6. Advancing Healthcare and Mental Health Support

Beyond medical diagnosis, AI can provide mental health support through intelligent applications that analyze behavioral patterns and offer preliminary psychological consultations. It is also used in remote patient monitoring, reducing pressure on healthcare facilities.

7. Advancing Translation Technology and Cross-Cultural Communication

Thanks to AI, real-time translation has become significantly more accurate and fluid, facilitating communication across different cultures, breaking down language barriers, and strengthening international understanding and cooperation among peoples.

8. Strengthening Cybersecurity and Data Protection

As cyber threats continue to multiply, AI assists in detecting cyberattacks in real time and reinforcing the protection of personal and governmental data, thereby reducing fraud and digital intrusions. AI represents the optimal solution for identifying cybersecurity threats, given its capacity for granular monitoring and automated activity analysis to identify risks (Hassan Nayef Mubarak, 2024).

2.2 Disadvantages of Artificial Intelligence

- Impact on the labor market: unemployment has grown markedly in recent years, particularly as AI and its programs have replaced humans in numerous digital occupations, such as writing, image editing, and data entry.
- Rising production costs: AI software and hardware require continuous development, and their maintenance demands considerable financial and human resources.
- Erosion of human skills: excessive dependence on technology renders individuals increasingly passive, delegating more and more tasks to automated systems, which gradually stifles human creativity.
- Ethical risks: AI necessitates the collection of vast quantities of personal data, leading to a significant erosion of privacy and creating the potential for this information to be exploited in unethical ways against individuals.
- Absence of genuine creativity: while AI is capable of performing an extensive range of tasks, it cannot truly replicate the human mind, and widespread reliance on it risks progressively extinguishing human creative potential.
- Infliction of serious harm on individuals, corporations, or nations — for example, through reputational damage via image manipulation or the non-consensual disclosure of sensitive personal material.
- Emergence of security threats: some actors exploit AI to launch cyberattacks and breach classified information, a phenomenon commonly referred to as cyber hacking.

3. Deepfake Techniques and Their Role in the Production of Electronic Rumors

3.1 Historical Background and the Evolution of Deepfake

Tracing the historical development of deepfake technology reveals that the term first appeared in 2017, when it began to be used extensively in the production of high-resolution fabricated video content. The technology emerged within specialized online communities, where AI algorithms were developed to modify video footage and digitally reconstruct facial features — making it increasingly difficult to distinguish authentic content from manipulated material. Deepfake gained widespread public visibility in the political domain when the media platform BuzzFeed published, on April 1, 2018, a video employing this technology to demonstrate how easily video footage could be manipulated, thereby bringing this technology to the attention of a broad global audience (Sayed, 2024, p. 487).

Its use continued to expand over successive years across virtually every domain worldwide, growing in direct correlation with advances in AI applications and the algorithms governing social media platforms — platforms that constitute fertile ground for the proliferation of rumors and fabricated content, given the intensive use of these platforms by diverse segments of society.

3.2 Characteristics of Deepfake

Grounding in Artificial Intelligence

Deepfake is fundamentally rooted in artificial intelligence — a field dedicated to developing systems capable of simulating human intelligence through the emulation of human cognitive capacities or through the independent development of technologies capable of solving complex problems. Its key applications include visual perception systems, natural language processing, machine learning, robotics, and specialized systems such as intelligent gaming engines. AI has demonstrated its effectiveness across numerous domains, including addressing complex technical and scientific challenges.

A Behavior Linked to Civilizational Development

The shift in criminal conduct from physical violence toward fraud and falsification reflects the perpetrator's capacity to leverage intellectual and technological tools — a capacity that is itself bound to the advancement of civilization, science, and modern communication technologies. Deepfake exemplifies a form of creative capability that requires a sophisticated technological environment to produce and deploy.

A Behavior of International Scope

Deepfake crimes are characterized by their transnational nature, owing to the use of interconnected software operating across global internet networks and the capacity to affect individuals and institutions in multiple countries simultaneously. This global dimension calls for coordinated international action to combat these crimes, given their potentially destabilizing impact on political and economic stability. Their effects extend to the economies and governance structures of states, undermining public order, threatening national integrity, and eroding public confidence in the stability of political systems on a broad scale (Mohammed, 2011, pp. 253–256).

A Behavior Predicated on Defamation

Deepfake represents a new era of fabrication in which truth is distorted through advanced technology. This technique is deployed to damage the reputations of public figures by producing manipulated videos that portray them saying or doing things they never actually said or did. In its early stages, the technology was used against prominent entertainers — inserting their likenesses into pornographic films in which they had never appeared — in order to tarnish their reputations (Mohammed, 2011).

3.3 Methods Used to Fabricate Rumors via Deepfake

- **Face Swapping**

This technique involves replacing one person's face in a video or image with another person's face using artificial intelligence, resulting in content that appears highly realistic. The process relies on analyzing facial features and substituting them with a three-dimensional model that aligns with the original facial expressions.

- Applications such as FaceApp and Reface are used to portray individuals at different ages or with altered physical appearances.
- A person's face may be digitally inserted into scenes from older films, effectively re-enacting those scenes without the need for any actual re-shooting.

- **Facial Expression and Motion Transfer**

This technique enables the modification of facial expressions and body movements in video footage, making an individual appear to be speaking or moving in a manner entirely different from the original — without any additional filming.

- **Deepfake Voice (Voice Cloning)**

Artificial intelligence is used to analyze the vocal characteristics of a specific individual, then construct a digital replica of their voice, enabling the generation of synthetic audio recordings in which the person appears to be speaking in their own authentic voice (Zakaria, 2023, p. 90).

- **Lip Sync Manipulation (Deepfake Lip Sync)**

This technique allows the modification of lip movements in a video to synchronize with a newly written script, making the individual appear to be uttering words entirely different from what they originally said.

Example: fabricated political videos in which world leaders appear to deliver statements they never actually made, potentially influencing political and economic decision-making.

- **Face and Body Morphing**

This technique involves superimposing one person's face onto another person's body, or digitally altering an individual's overall physical appearance. It relies on biometric data analysis and the digital reconstruction of that data with a high degree of precision.

Example: manipulating images of public figures and inserting them into situations they were never actually part of, which may have serious consequences for their reputations.

3.4 Principal Applications

The following are among the most widely used applications for producing digital content and fabricating rumors for circulation across social media platforms:

- **Zao:** A Chinese application that allows users to replace their faces with those of characters from popular films or video clips. Its interface is notably user-friendly: the user simply uploads a personal photograph, selects the desired clip, and the face is automatically integrated.
- **FaceApp:** A widely popular application that enables users to apply a variety of AI-powered effects to their photographs, such as simulating different ages or altering gender appearance. Its main interface offers intuitive options for editing photos and adding effects.
- **Reface:** Formerly known as Doublicat, this application allows users to replace their faces with those of celebrities in short video clips and GIFs. It features a modern, easy-to-use interface with an extensive content library.
- **Speak Pica:** An application that makes still images appear to speak using artificial intelligence. Users can input text or record audio, and the application animates the subject's lips to synchronize with the vocal content.
- **DeepFaceLab:** An open-source tool used to create fabricated videos through face replacement. It is considered one of the leading tools in this domain but requires advanced technical knowledge for effective use.
- **Reflect:** An application that enables face replacement in images using AI, with a strong emphasis on preserving visual details and ensuring realism. Its interface is straightforward and intuitive.

- **Web Deep Fake:** An internet-based service that uses machine learning algorithms to replace faces in video clips. Users upload their videos and images, and the algorithm processes them to produce an edited output.
- **Instagram Deep Fake Bot:** An Instagram account that allows users to generate deepfake images by submitting their photographs, after which the bot returns the images with deepfake modifications applied.
- **Deep Fake Studio:** An application that enables face replacement in film scenes, music videos, and other content, with the option to use deep learning to enhance results. It offers multiple tools to refine the editing process.
- **Deep-Live-Cam:** A software suite that allows the real-time application of deepfake techniques during video calls. It can extract a person's face from a single photograph and track their posture, lighting, and expressions via webcam. Following its online release, the application rapidly gained popularity and reached the top of the download charts on GitHub, particularly given that it is available free of charge (Asharq.com, 2024).

These applications represent the most widely used tools in the field, primarily because the majority are simple to operate, easy to download, and in many cases free of charge. A wide range of additional applications also exist, each suited to specific needs and objectives — whether for fabricating images of specific individuals, producing videos in which they appear to speak, or other forms of manipulated content.

4. Rumors and Their Impact on the Individual and Society

Anyone who regularly browses social media today is immediately aware of the sheer volume of information circulating in real time — whether in the form of text, images, or videos featuring prominent public figures or ordinary citizens. This reality constitutes a direct facilitating factor in the spread of misinformation and the ease with which fabricated allegations can be disseminated, particularly given the remarkable technological advances in content creation and the vast capabilities that artificial intelligence tools now provide.

Among the most significant consequences of the spread of rumors, the following may be identified:

- **Psychological effects:** the inducement of anxiety, fear, frustration, and a pervasive sense of insecurity.
- **Reputational damage:** the wrongful targeting of individuals, the violation of their dignity, and the destruction of their social and professional lives.
- **Erosion of critical awareness:** rendering individuals vulnerable to deception and the falsification of reality.
- **Destabilization of security and stability:** generating panic and confusion, and fueling discord among different segments of society.
- **Social fragmentation:** weakening social bonds among people and cultivating an atmosphere of mutual suspicion and distrust.
- **Economic harm:** precipitating misguided financial decisions, such as bank runs or market crises triggered by false information.
- **Undermining national identity:** weakening citizens' sense of belonging and eroding confidence in state institutions.

In light of the pervasive spread of rumors — particularly within digital spaces — and their far-reaching impact on both individuals and communities, it is imperative to develop effective solutions and strategies to counter them and limit their reach. The following approaches are proposed:

AI-Based Detection Applications: these rely on sophisticated algorithms to analyze information and flag fabricated news automatically and in real time, significantly outpacing traditional human fact-checking teams in both speed and scale.

Digital Tracking: these solutions go beyond mere rumor detection to actively track its spread, trace its source, and verify its components in a systematic and immediate manner. Among the most notable examples is the Emergent platform — part of a research project affiliated with the Tow Center for Digital Journalism at Columbia University — which affixes labels to rumors indicating whether they are confirmed, false, or unverified. Clicking on a labeled item reveals its source, the extent of its circulation, and additional relevant information.

Rumor Control Centers: these are observatories equipped with the technical tools and applications necessary to monitor cyberspace and detect rumors, particularly during periods of crisis and emergency. Researcher Onook, from the University of Warwick (UK), highlighted in his study on the spread of rumors via social media the critical importance of such centers in debunking disinformation and ensuring that citizens receive accurate, timely information through various media and communication channels — including websites, social networks, real-time feeds, email, and text messaging — in addition to traditional media. He described this flow of accurate information as a counter-current that helps contain the spread of rumors, referencing the positive role played by the Rumor Control Center of the U.S. Federal Emergency Management Agency during Hurricane Sandy.

Participatory Counter-Measures: this approach actively engages users themselves in the fight against rumors by raising public awareness and encouraging individuals to report suspicious content. Facebook adopted this strategy by adding guidance for users to identify and flag fake news within its mobile application across 14 countries worldwide, enabling users to mark such content and submit it directly to bodies responsible for fact-checking and verification (Al-Fattah, 2017).

Conclusion

The world has witnessed a wave of technological transformation — particularly with regard to the use of modern technologies such as artificial intelligence, algorithms, and robotics — accompanied by the emergence of new behavioral patterns commensurate with this profound scientific progress. As a result, the rapid spread of information has become the norm, regardless of its veracity. The electronic rumor represents one paradigmatic example among many of the phenomena that have emerged as direct consequences of this technological determinism. Deepfake technology, in particular, has dramatically amplified the reach and impact of misinformation, affecting diverse segments of society. Given the significant harms and consequences that rumors pose to both individuals and communities, it is essential that serious strategies be developed to confront them and curb their proliferation.

References

- Abd al-Hadi, Z. (2020). Artificial intelligence and expert systems in library science (1st ed.). Cairo: The Academic Library.
- Al-Fattah, F. A. (2017). Combating rumors in cyberspace. Canadian University
- Al-Sharif, M. S. (2022). The crime of revenge pornography via deepfake technology and criminal liability. Egypt
- Habib, M. A. (2019). Artificial intelligence. Cairo: The Arab Group for Training and Publishing.
- Hassan Nayef Mubarak, A. (2024). The role of artificial intelligence in enhancing cybersecurity (Vol. 32). Journal of University Studies for Comprehensive Research.
- Jawad, A. (2024). The phenomenon of the electronic rumor. Journal of Knowledge [Majallat al-Ma'rifa].
- Khaddour, L. (2023). Some applications of deepfake technology and their deployment in contemporary marketing and promotion (Vol. 02). Damascus University Journal of Engineering Sciences.

- Mohammed, F. A. (2011). Civil liability arising from the unlawful use of artificial intelligence applications: Deepfake technology as a model. *Journal of Legal Research [Majallat al-Buhuth al-Qanuniyya]*.
- Sayed, A. A. (2024). *The criminal confrontation of deepfake technology*. Egypt: Assiut University.
- Siham, S. M. (2024). *The use of artificial intelligence in scientific research and its contribution to achieving sustainable development (Vol. 03)*. Algeria: Hawliyyat Journal.
- Zakaria, B. S. (2023). *The impact of deepfake technology on media content (Vol. 5)*. Algeria: Higher Military School of Information and Communication.
- A new deepfake tool for real-time face replacement during video calls. (2024). *asharq.com*. Retrieved from <https://www.asharq.com>