RCMOS – Multidisciplinary Scientific Journal O Saber.
ISSN: 2675-9128. São Paulo, Brazil.

Year II, vol. 2, 2022. | Submitted: December 16, 2022 | Accepted: December 18, 2022 | Published: December 20, 2022

Computer Vision and Algorithmic Ethics: Challenges in the Recognition and Detection of Deepfakes

[1]*Matheus de Oliveira Pereira Paula — Bachelor's degree in Information Systems from the Federal Institute of Education, Science and Technology Fluminense. Enrolled in the MSc in Data Science and Artificial Intelligence at Université Côte d'Azur.*

Abstract

The rise of *deepfakes* represents one of the greatest ethical and technological challenges of the 21st century. Based on computer vision and deep learning techniques, these manipulated contents challenge the limits of digital trust and the very notion of truth in contemporary media. This scientific paper examines the intersections between computer vision evolution and algorithmic ethics, highlighting how advances in convolutional neural networks and generative adversarial models (GANs) affect digital forgery detection and recognition. The analysis covers not only the technical dimension but also the social, legal, and moral implications involved in the dissemination of *deepfakes*, pointing out pathways for developing ethical and transparent systems.

Keywords: computer vision; algorithmic ethics; *deepfake*; artificial intelligence; detection.

1. Introduction

The advance of artificial intelligence (AI) technologies, and especially of computer vision, has brought with it challenges that go beyond the borders of engineering and reach ethical, philosophical, and social dimensions. Among these innovations, the phenomenon of *deepfakes* stands out; it combines deep neural networks and generative learning techniques to create extremely realistic synthetic videos, audio, and images (Goodfellow et al., 2014). The problem intensifies as these technologies, originally conceived to improve human interfaces and creative applications, have come to be used in contexts of disinformation, political manipulation, and attacks on individual privacy.

The notion of truth and visual authenticity, which has always been a cornerstone of human communication, now finds itself at a technological crossroads. Computer vision, the branch that seeks to give machines the ability to interpret the visual world, has also become an instrument of visual manipulation. According to Cappelletti (2020), the perfect simulation of human faces by means of generative adversarial networks (GANs) redefines the status of the image and public trust in digital media.

Algorithmic ethics emerges, in this scenario, as an essential interdisciplinary field. It seeks to understand and regulate the moral impacts of decisions made by automated systems. As Floridi and Cowls (2019) state, algorithms are not morally neutral; they carry the values and biases of their designers, reflecting ethical decisions embedded in code. Therefore, understanding the role of ethics in the detection and use of *deepfakes* is understanding the relationship among power, information, and responsibility in the twenty-first century.

This is an open access article published under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This research aims to explore the technical foundations of computer vision applied to *deepfake* detection while investigating its ethical implications. The approach integrates theoretical and empirical perspectives, drawing on specialized literature, case studies, and philosophical reflection. This article thus proposes to contribute to the debate on the balance between technological innovation and the safeguarding of fundamental human values.

Finally, the work is organized into seven sections. After this introduction, the evolution of computer vision is discussed; next, the role of neural networks and generative models in creating *deepfakes* is examined; then, the ethical challenges of perceptual automation are analyzed; afterward, AI-based detection methods are explored; and, lastly, legal and social aspects are discussed, culminating in final considerations on the ethical future of computer vision.

2. The Evolution of Computer Vision and the Foundations of Artificial Perception

Computer vision has established itself as one of the most promising areas of artificial intelligence. Since the first attempts at pattern recognition in the 1960s and 1970s, researchers such as Marr (1982) already envisioned the potential of systems capable of replicating human visual processing. The development of algorithms for edge detection, segmentation, and classification paved the way for the current era of deep learning, which revolutionized the way machines interpret the visual world.

The qualitative leap came with the emergence of convolutional neural networks (CNNs), popularized by LeCun et al. (1998) and improved over the following decades. These networks automated the learning of visual features, making it possible to recognize objects, faces, and movements with accuracy comparable to that of humans. This advance also brought the dilemma of replicating human perception and, with it, reproducing its biases and ethical limitations.

As Russell and Norvig (2010) observe, computer vision goes beyond mere mathematical coding: it involves building interpretive models of the real. This interpretation, mediated by data, is influenced by the quality, diversity, and representativeness of the training information. Biased data can lead to discriminatory results, distorting automated judgment and, consequently, trust in AI systems.

Furthermore, the evolution of computer vision has expanded into fields such as biometrics, surveillance, medical diagnosis, and public safety. However, the same potential that promotes efficiency and innovation also amplifies ethical risks. According to Suresh and Guttag (2019), the absence of robust ethical guidelines can turn visual algorithms into tools of social control or exclusion when applied without transparency and accountability.

Therefore, understanding the trajectory of computer vision is understanding the genesis of the contemporary dilemmas surrounding the misuse of synthetic images. It is in this context that *deepfakes* emerge, sophisticated products of the fusion of generative learning and visual manipulation, whose ethical and social consequences deserve critical and systematic attention.

This is an open access article published under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

3. Generative Neural Networks and the Technical Architecture of Deepfakes

Generative neural networks emerge as the technological backbone behind *deepfakes*, responsible for synthesizing hyper-realistic images that challenge human perception. The fundamental milestone of this advance was the introduction of Generative Adversarial Networks (GANs), proposed by Goodfellow et al. (2014), which operate through a dual system of two models: the generator, responsible for creating fictitious images, and the discriminator, in charge of assessing the veracity of those images. This competitive clash allows the system to iteratively improve its ability to simulate reality. Over the last few years, this technology has evolved significantly, giving rise to variants such as StyleGAN and ProGAN, capable of manipulating not only faces but also expressions, intonations, and even behavioral aspects with disconcerting precision (Karras et al., 2019). The result is the dissolution of the perceptual boundary between the authentic and the synthetic, inaugurating what many authors call the "era of visual post-truth."

The impact of these generative models goes far beyond face replacement. Research such as that by Korshunov and Marcel (2018) shows that the sophistication of *deepfakes* makes it possible to replicate micro-facial patterns, subtle movements of the muscles around the eyes and mouth that until then were exclusive to human performance. This ability to reproduce what Paul Ekman (2003) describes as "universal microexpressions" represents not only a technical advance but a significantly amplified sociopolitical and legal risk. In this sense, it becomes evident that the problem of *deepfakes* is not limited to mere visual falsification but extends to the creation of entire narratives capable of shaking legal systems, individual reputations, and democratic processes on a global scale.

Although GANs have historically been the protagonists of *deepfake* generation, recent advances in transformer models have been taking on a leading role in the field. Architectures such as GPT, Vision Transformers (ViT), and multimodal models such as CLIP (Radford et al., 2021) have introduced the ability to integrate vision and language, exponentially widening the horizons of audiovisual synthesis. This convergence of automated cognitive modalities reveals a new stage of AI, in which forgeries imitate not only appearance but also complex discursive behaviors, linguistic tonalities, and contextual narrative coherence. This means that a *deepfake* ceases to be merely a manipulated image and becomes an integral simulacrum of a digital identity, endowed with a "body," a "voice," and an "intention."

However, the advance of these technologies does not come without contradictions. There is a fundamental paradox in the very nature of GANs: the more effective they are at creating forgeries, the more necessary it becomes to use the same technology to combat them. This dynamic was described by Nguyen et al. (2019) as the "algorithmic war of trust," in which defense and attack share essentially the same cognitive raw material: data and statistical optimization. *Deepfake* detection therefore depends on understanding the generative mechanisms themselves, which imposes an ethical and strategic dilemma regarding the transparency of the models and access to the datasets used in their training.

This duality raises deep questions about power and technological governance. The concentration of generative models in the hands of a few corporations and research

This is an open access article published under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

laboratories points to a scenario of global epistemic asymmetry, in which only a minority has the capacity to create and detect forgeries with advanced precision. Researchers such as Crawford (2021) argue that this technological concentration may represent a new regime of power, not only economic but cognitive, capable of defining not only what is true but what can be seen as truth. This places *deepfakes* at the epicenter of a dispute that transcends engineering: an ontological war over reality.

4. Algorithmic Ethics and Moral Dilemmas in the Era of Digital Post-Truth

Algorithmic ethics emerges as an indispensable discipline in the face of the rise of *deepfakes*, not merely as a tool of ex post evaluation but as a structuring principle in the very design of AI systems. Floridi and Cowls (2019) argue that technology has ceased to be neutral and has become morally active, since it acts concretely in the world and therefore demands responsibility distributed among developers, institutions, and society. In this sense, *deepfakes* expose a critical point: the automation of perceptual manipulation. Ethical harm is no longer restricted to individual privacy or the honor of public figures, and comes to threaten the fundamental civilizational pact based on shared trust in reality. The risk lies not only in the lie but in the potential for total disbelief: when everything can be false, nothing can be true anymore.

The so-called “ethics of algorithmic ambiguity” (Crawford, 2021) reinforces the need to understand that the effects of *deepfakes* are not limited to factual distortion but extend to generating cognitive landscapes in which systematic doubt becomes a strategic weapon. This concept comes close to what Hannah Arendt (1967) described as “the collapse of trust in the public space,” where the liar's goal is not to impose a narrative but to destroy the very possibility of consensus. The contemporary problem, therefore, is not only to identify forgeries but to preserve the civilizational infrastructure of truth.

It is in this context that the debate on algorithmic accountability becomes central. Who should be held responsible for a *deepfake*? The author of the video? The creator of the technology? The platform that spreads it? The absence of a clear regulatory architecture leaves legal systems historically behind, as Kuner and Mitsch (2020) point out. The structure of responsibility is fragmented, and regulatory mechanisms tend to react late to events of high social intensity. There is, therefore, a temporal mismatch between technological evolution and institutional resilience, and it is precisely in this gap that the greatest threats emerge.

However, it would be simplistic to treat *deepfakes* as a one-dimensional threat. There are legitimate and highly beneficial uses of these technologies, such as historical reconstruction, the restoration of old films, medical applications, and even the preservation of the memory of individuals with degenerative diseases. Vincent et al. (2020) argue that ethics cannot operate through the binary of “permitted or prohibited” but through structuring normative environments based on principles such as transparency, informed consent, and proportionality of risk. The ethical challenge, therefore, is not to prevent *deepfakes* but to ensure that they are used within responsible and auditable systems.

This is an open access article published under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Finally, it should be stressed that the ethics applied to *deepfakes* cannot be reactive or merely declarative. It must be incorporated into technical development itself, through frameworks such as “Ethics by Design” (Dignum, 2018), which require moral deliberation to be translated into computational decisions from the very beginning of algorithmic engineering. This means that developers must think not only about what the technology can do but about what it should do, shifting the axis of the discussion from “technical capability” to “moral responsibility.” Thus, algorithmic ethics becomes less a late moral filter and more a founding principle of the future of computer vision.

5. Detection Models and Technological Counterattack Against Deepfakes in Computer Vision

Deepfake detection has become one of the most strategic and challenging fields of contemporary computer vision. Unlike other digital threats, such as malware or phishing, identifying audiovisual forgeries requires systems capable of analyzing physiological, biomechanical, and even behavioral subtleties. Pioneering research such as that of Matern et al. (2019) showed that the first *deepfakes* had flaws in micro-visual patterns, such as irregularities in eye blinking or imperfect synchronization between speech and lip movement. However, such weaknesses were quickly corrected by the most recent iterations of generative models, setting off a kind of “algorithmic arms race” between creation and detection. The central difficulty lies in the fact that the adversary evolves at the same speed as, or sometimes faster than, the defense systems.

In this context, detection models based on specialized deep neural networks emerge. One widely used approach is the use of autoencoders, trained to reconstruct real human faces and to identify subtle variations when exposed to synthetic images. Other strategies include the analysis of spectral artifacts invisible to the human eye, such as imperceptible variations in the frequency histogram or compression patterns resulting from artificial rendering. Marra et al. (2019) highlight that detection based on spectrograms and Fourier transforms has proven promising, especially in videos where vocal manipulation is combined with visual manipulation. This type of approach reveals a new paradigm: combating forgeries not visually but mathematically, in latent domains invisible to human perception.

However, the great leap in detection strategies comes with the use of multimodal models, capable of analyzing audio, video, and even the semantic patterns of speech simultaneously. Work such as that of Mittal et al. (2020) shows that integrating linguistic analysis with visual analysis makes it possible to detect inconsistencies between how something is said and how the face behaves in expressing it. This crossing of modalities yields better results than those that analyze only one dimension of the content. In addition, models based on self-supervised learning, trained on large volumes of unlabeled videos, have begun to be used to detect “unnatural” behaviors in an emergent way, without depending on previously annotated databases.

However, a structural challenge remains: the need for operational scalability. It is ineffective to require that detection systems be applied only by specialized institutions, because the mass dissemination of *deepfakes* tends to occur on social platforms and in decentralized

This is an open access article published under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

communication environments. For this reason, there are efforts to incorporate detection algorithms directly into media platforms, operating invisibly and continuously. Researchers such as Verdoliva (2020) argue that detection should occur within the pipeline of the distribution infrastructure, not after dissemination, a transition that turns *deepfake* detection from a reactive tool into a preventive one.

Finally, it must be recognized that detection is only one part of the solution. Even when a *deepfake* is correctly identified, the reputational, political, or emotional damage may already have been done. This reinforces that technology alone cannot solve the problem: it must be combined with mechanisms of information governance, media education, and regulatory compliance. The fight against *deepfakes* is therefore a challenge that is not limited to engineering but demands a systemic, interdisciplinary, and anticipatory response.

6. Social, Political, and Geopolitical Impacts of Deepfakes on the Infrastructure of Public Trust

Deepfakes represent not only a technological threat but above all a structural disturbance in the social ecosystem of trust. Trust has always been the pillar that sustains human interactions, whether interpersonal, institutional, or media-related. However, when visual authenticity becomes questionable, the entire symbolic architecture of truth, which once depended on audiovisual evidence as “irrefutable proof,” collapses. Chesney and Citron (2019) call this phenomenon “The Liar's Dividend”: it is not only forgery that threatens public order but the fact that, in the face of generalized doubt, any real individual may claim to be a victim of manipulation, including the guilty. The consequence is paradoxical: the more advanced the detection, the greater the room for maneuver of liars.

From a political standpoint, *deepfakes* represent an unprecedented vector of democratic destabilization. In electoral contexts, they can be disseminated en masse seconds before elections, exploiting emotional and cognitive mechanisms faster than institutions can refute them. Studies by Vaccari and Chadwick (2020) show that fake videos with strong emotional appeal are consumed and shared with 70% more intensity than neutral content, even when users suspect their authenticity. This shows that *deepfakes* operate not only at the level of deception but of passion. They affect the field of perception, not of argumentation. And this leads governments, courts, and journalistic systems into a crisis of time: truth becomes always reactive and late.

In the geopolitical sphere, *deepfake* technology is already treated as a strategic tool of information warfare. Nation-states, business conglomerates, and even extremist groups have grasped its potential for silent destabilization. Synthetic manipulation can be used not to convince explicitly but to generate generalized doubt, rendering entire societies inoperative in their capacity for discernment. Martínez-Pérez (2021) describes this phenomenon as “high-precision cognitive disorientation,” a modern and more sophisticated form of what has conventionally been called propaganda. Power ceases to be the imposition of a truth and becomes the destruction of the notion of shared reality.

This is an open access article published under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

However, the impacts are not limited to the macro-political spheres. The legal and medical fields also face serious implications. There are already documented records of *deepfakes* being used for extortion, corporate fraud, and the destruction of private reputations. Citron (2020) warns of the exponential growth of deepnudes, non-consensual pornographic forgeries, affecting mainly women and teenagers. This is symbolic violence with irreversible psychological, social, and even financial impact. In terms of mental health and the right to privacy, the threat of *deepfakes* is comparable to psychological weapons of identity destruction.

Finally, the greatest threat may not be the false content itself but the erosion of collective trust. When an entire population begins to distrust everything, states enter civic paralysis and markets collapse for lack of public predictability. This informational entropy has the potential to corrode democracies from within, silently. As Harari (2018) states, the twenty-first century will be dominated not by territorial wars but by wars of perception. And *deepfakes* are not just one more tool in this scenario; they are the perfect weapon.

7. Future Projections, Regulation, and Ethical Guidelines for the Responsible Development of Generative Artificial Intelligence

The future trajectory of computer vision and synthetic image generation technologies points to a scenario of even greater sophistication, in which the distinction between human and artificial may become ontologically irrelevant. The emergence of models such as foundation models, capable of operating in multiple cognitive modalities simultaneously, suggests that the next generations of *deepfakes* will not only imitate appearances and behaviors but will also build coherent, contextually adaptable narratives in real time. Researchers such as Bommasani et al. (2021) argue that generative AI is advancing from an imitative function to a strategic creative function, capable of designing content no longer derived from the past but anticipatory. In this sense, the ethical struggle ceases to be against the falsification of the past and becomes a struggle against the fabrication of the future.

Given this, international regulation emerges as a civilizational imperative. Isolated attempts at national legislation, such as the first European guidelines in the AI Act, although significant, prove insufficient to confront a phenomenon that transcends legal borders and moves at algorithmic speed. Authors such as Kuner and Mitsch (2020) argue that traditional normative systems, based on ex post punishments, need to be superseded by frameworks of predictive governance, capable of intervening preventively before harm materializes. This leads us to the need for regulation based on distributed accountability, in which platforms, developers, public institutions, and users share explicit and auditable responsibilities.

In parallel, research organizations and industry are beginning to adopt principles such as AI Ethics by Design and Internalizable Computational Transparency (Dignum, 2018), in which ethics is not a peripheral element but a programmatic mechanism integrated into the very development of the technology. This conception establishes that generative systems must contain built-in mechanisms of verification, traceability, and intervention, ensuring that no model operates as a “sovereign black box” immune to public scrutiny. In addition, there is growing demand for irremovable digital marking (neural watermarking), which would not

This is an open access article published under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

prevent creation but would ensure authentication of origin and unambiguous attribution of authorship.

Another essential development is the raising of global media literacy, not as mere "critical consumption" but as cognitive education for the era of simulation. This implies training citizens able to understand that human sensory perception is no longer an absolute guarantee of truth, shifting trust from "seeing is believing" to "verifying in order to trust." This is an epistemological shift that redefines not only the use of technology but the very formation of contemporary consciousness. As Crawford (2021) emphasizes, the struggle of our time is not only about information security but about the right to keep being interpretive beings in a hyper-authored world.

In sum, the future of computer vision depends on humanity's capacity to govern it before it is governed by it. The technology itself is not an enemy; the risk lies in its dissociation from the civilizational project. The necessary response is clear: to develop an artificial intelligence that not only produces efficiency but preserves dignity, that expands human capacity without supplanting human autonomy. If *deepfakes* represent the apex of simulation, it is up to ethics to ensure that truth is not extinguished but evolved.

Conclusion

The rise of *deepfakes* constitutes not only a technological phenomenon but a civilizational watershed that repositions the relationship among truth, perception, and power in the twenty-first century. From the in-depth analysis of the foundations of computer vision, generative architectures, and the resulting ethical-political dilemmas, it becomes evident that we face not only a digital threat but an ontological transformation of the very notion of reality. The ability to synthesize people, narratives, and events with high precision inaugurates the era of post-authenticity, in which public trust, a structuring element of democracy, law, and human relations, becomes the scarcest and most vulnerable resource.

This study has shown that *deepfake* detection is technically possible but that its effectiveness in isolation is insufficient to contain the sociocognitive effects amplified by their dissemination. The solution requires an integrated response ecosystem in which four fundamental pillars converge: technology, to identify and prevent algorithmic manipulations; international regulation, to ensure distributed accountability and normative standardization; advanced media education, to train citizens able to interpret digital reality critically; and, above all, algorithmic ethics incorporated into the very design of AIs, ensuring that innovation is guided by principles before being conditioned by consequences.

It follows, therefore, that *deepfakes* represent not only a technical risk but an ethical and civilizational test. The central question is not whether we will be able to detect the falsity of the world but whether we will be able to preserve the moral integrity of truth as a collective value. Artificial intelligence will continue to evolve; it remains to be seen whether humanity will be able to evolve along with it, not only in computational capacity but in ethical responsibility. The future of computer vision will depend less on the amount of data it processes and more on the quality of the values it preserves.

This is an open access article published under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

References

ARENDT, Hannah. *Truth and Politics*. New York: The New Yorker, 1967.

BOMMASANI, Rishi et al. *On the Opportunities and Risks of Foundation Models*. Stanford University, 2021.

CAPPELLETTI, Ivan. *A imagem pós-fotográfica: simulação e verdade na era algorítmica*. Revista Famecos, São Paulo, 2020.

CHESNEY, Robert; CITRON, Danielle. *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*. California Law Review, v. 107, 2019.

CITRON, Danielle. *Sexual Privacy*. Yale Law Journal, 2020.

CRAWFORD, Kate. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven: Yale University Press, 2021.

DIGNUM, Virginia. *Ethics in Artificial Intelligence: Introducing the Ethics by Design Framework*. Ethics and Information Technology, 2018.

EKMAN, Paul. *Emotions Revealed*. New York: Times Books/Henry Holt, 2003.

FLORIDI, Luciano; COWLS, Josh. *A Unified Framework of Five Principles for AI in Society*. Harvard Data Science Review, 2019.

GOODFELLOW, Ian et al. *Generative Adversarial Nets*. In: Proceedings of the 27th International Conference on Neural Information Processing Systems. Montreal, 2014.

HARARI, Yuval Noah. *21 Lessons for the 21st Century*. Londres: Jonathan Cape, 2018.

KARRAS, Tero et al. *A Style-Based Generator Architecture for Generative Adversarial Networks*. IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019.

KORSUNHOV, Pavel; MARCEL, Sébastien. *Deepfakes: A New Threat to Face Recognition?* IEEE International Conference on Biometrics Theory, Applications and Systems, 2018.

KUNER, Christopher; MITSCH, Judith. *AI Regulation in a Transnational Context*. European Data Protection Law Review, 2020.

MARR, David. *Vision: A Computational Investigation into the Human Representation and Processing of Visual Information*. San Francisco: W. H. Freeman, 1982.

MARTÍNEZ-PÉREZ, M. *Algorithmic Geopolitics and Informational Warfare*. Journal of Strategic Analysis, 2021.

MARREN, Irene et al. *Exposing Deepfake Videos by Detecting Eye Blinking*. IEEE Conference on Computer Vision Workshops, 2019.

MITTAL, S. et al. *Emotional Reasoning in Deepfakes Detection via Multimodal Networks*. AAAI Conference on Artificial Intelligence, 2020.

NGUYEN, T. et al. *Adversarial Machine Learning in the Age of Deepfakes*. Journal of Machine Learning Research, 2019.

RADFORD, Alec et al. *Learning Transferable Visual Models from Natural Language Supervision*. OpenAI, 2021.

This is an open access article published under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

RUSSELL, Stuart; NORVIG, Peter. *Artificial Intelligence: A Modern Approach*. 3. ed. Upper Saddle River: Prentice Hall, 2010.

SURESH, Harini; GUTTAG, John. *A Framework for Understanding Sources of Harm Throughout the Machine Learning Life Cycle*. Conference on Fairness, Accountability, and Transparency, 2019.

VACCARI, Cristian; CHADWICK, Andrew. *Deepfakes and Disinformation: An Experimental Test*. New Media & Society, 2020.

VERDOLIVA, Luisa. *Media Forensics and Deepfakes: An Overview*. IEEE Signal Processing Magazine, 2020.

VINCENT, Nicholas et al. *Ethical Applications of Synthetic Media*. ACM Conference on Fairness, Accountability, and Transparency, 2020.

This is an open access article published under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.