Opinion Paper

45/2025 06/06/2025

Estíbaliz Garcia Huete et al.*

AI & serverless systems in war disinformation via LUTs: impact and ethics

AI & serverless systems in war disinformation via LUTs: impact and ethics

Abstract:

The present research consists of the creation and reflection on the role of Generative Artificial Intelligence and its impact on the informational and propagandistic world, with the aim of understanding and mitigating the impact of misinformation in the digital age. The research will be supported by an experiment in which a Generative AI will produce war-themed images from scratch, applying (Look Up Tables) LUTs to these images to increase their realism to a point where they can be perceived as authentic, which could contribute to disinformation campaigns.

The development of technological tools capable of identifying and countering these threats is crucial in a context where the integrity and veracity of information are fundamental elements for security and social stability.

Keywords:

Artificial Intelligence, Propaganda, Fake News, Disinformation, Social Media

How to quote:

GARCÍA HUETE, Estíbaliz. et al. *AI & serverless systems in war disinformation via LUTs: impact and ethics.* Opinion Paper. IEEE 45/2025.

Introduction

Nothing that happens in history is understood without a basis of propaganda and disinformation. In war contexts, propaganda and disinformation intensify, spreading faster and more aggressively as new media platforms emerge to influence public sentiment.

The advent of Generative Artificial Intelligence has exacerbated this issue. Within less than two years, AI has been trained to create photos and videos from scratch with a worrying degree of realism, posing a threat to information security and public opinion. This leaves information professionals feeling like they are in a race against time to analyse the provenance of such creations and verify their authenticity. Social networks like X (formerly Twitter) and Instagram facilitate the virilization of information, including false information, through features like retweeting and sharing. Similarly, on TikTok, a popular platform among younger users, videos are often shared without verification of their origin, context, or authenticity.

Generative Artificial Intelligence (AI) has gained increasing relevance due to its use and propagation in diverse digital platforms, including media and social digital platforms, including media and social networks. The distrust of traditional media, the drift of hegemonic discourses and the rise of Artificial Intelligence push us into a maelstrom full of uncertainty and fear that leads to a reflection on its use in the current context, and how and at what pace its impact on society may evolve in times to come. Due to its relevance in current war scenarios, where public perception can be manipulated to influence political decisions or the collective morale of a society, we thought it necessary to delve into the role of artificial intelligence in war conflicts and its propagandistic influence at the media and political level.

In recent years, the Armed Forces have recognized the cognitive domain as a determining factor. The reason is that this domain of perceptions, emotions, thoughts and beliefs, transcends the traditional ones (terrestrial, maritime, aerospace and cyberspace). In the military domain, understanding and influencing the cognitive dimension is crucial for operational effectiveness, as outcomes depend not only on technological or kinetic capabilities but also on psychological influence. For this reason, both metaphorically and literally, the cognitive domain constitutes a new battlefront, where perception, narratives,

propaganda and information become as effective weapons as conventional media.[1]

We have measured its impact thanks to an experiment that consists of a generative AI that can create war images through patterns and algorithms. The computation of these images is done in a distributed composition with serverless architectures to improve efficiency and reduce costs. LUTs have been applied to increase their perceived realism. These images have been evaluated by the human eye to measure their persuasiveness, adding automated detection tools to assess the ability of current systems to identify the generation (i.e., non-authenticity) of these images. This approach will help to effectively evaluate the potential of Generative AI in the application of manipulating the population, and to contribute to the debate on the ethical implications of generative AI in the field of disinformation.

This work is the result of the collaboration of research groups belonging to two academies of the Complutense University of Madrid: The Faculty of Information Sciences and the Faculty of Computer Science. Each of these groups brings a multidisciplinary approach that enriches the development of the work presented here. The group from the Faculty of Information Sciences focuses on the communicative and social aspects of misinformation, while the group from the Faculty of Computer Science is responsible for measuring color parameters (such as histograms), analysing image differences, implementing the AI model technically, and managing the distributed computing infrastructure needed for the large-scale experiment.

Where do we start from?

Most of today's social networks were born at the beginning of the new millennium, in the first decade of the 2000s. They range from media accounts to users with a certain reputation, who owe their popularity to their high level of interaction and their large number of followers, and who in some cases can be contacted for the promotion of fake news. This promotion of fake news or hoaxes is often used for an ironclad and blind defense of certain ideas or positions. Due to the algorithms that govern these social

[1] Peco Yuste, Miguel, “Implicaciones del ámbito cognitivo en las Operaciones Militares” Instituto Español de Estudios Estratégicos, pp. 109-137, (2020)

networks, the appearance of so-called “ideological bubbles” on the user's timeline is favored. This phenomenon, in which users end up receiving content exclusively from others close to their ideological sphere, is already widespread.

For example, Twitter and Facebook were mostly very similar sites. Both offered users to share images, videos and news with other people. Previously, X/Twitter arguably offered users more control over their information filters and greater transparency regarding content presentation compared to Facebook, where such control was perceived as more limited.

Generative artificial intelligence (AI) is defined as: “a scientific and technological discipline that seeks to create systems capable of solving tasks that normally require human intelligence”[2].

It could be a very useful tool for propaganda purposes and promotion of speeches and ideas. That is why it has been proposed to develop and train a generative AI model that creates war-themed images that are perceived as real.

How is it done?

The generative AI used creates war-themed images from a series of patterns and algorithms. To measure and enhance its impact, a study was designed applying LUTs to the generated images. This allows for assessment of their perceived authenticity and the potential risk of their use in disinformation campaigns. LUTs replicate color patterns, saturation and a dynamic range typical of cameras used by war correspondents, which adds an additional layer of complexity to the detection of this type of manipulations, usually generated in today's social networks.

The correlation between certain color patterns, study of figures and environments and the likelihood of images appearing real could be established by the success and recognition of such an experiment. This would give rise to new research on the dynamics of media manipulation. Investigating a serverless Artificial Intelligence framework in this

[2] Franganillo, Jorge, “La inteligencia artificial generativa y su impacto en la creación de contenidos mediáticos” methaodos.revista de ciencias sociales, 2023, vol. 11, no 2, p. 10.

experiment is expected to significantly advance both the creation and identification of fake news. That is why the following objectives have been proposed:

A substantial contribution to the debate on the ethical, political and economic consequences and possible countermeasures to prevent the manipulation of information in the digital age will be elaborated. This will involve raising public awareness through images created about what the current context of generative AI is, highlighting its main advances and studying its future levels of perfection.

Optimized LUT techniques: Integrate and refine the use of color lookup tables to improve the perception of authenticity in AI-generated images.

Serverless infrastructures will be implemented: Deploying and evaluating serverless architectures for the creation and subsequent analysis of images and false data on a large scale.

To disclose how Generative Artificial Intelligence works, including its main features and operational mechanisms.

Distributed computing is a field of computer science that focuses on using multiple computers to work together as if they were a single system. Serverless is a model of computing (currently, it is the most advanced that exists) in the cloud in which the infrastructure is managed by the cloud provider, allowing developers to focus solely on writing and deploying code. It consists of large numbers of processors that are not connected to each other, and all solve the same problem at the same time. Such a computing model has more fault tolerance, and more problems can be solved in less amount of time.

In the case of the experiment, two tools provided by Amazon Web Service have been used: AWS Lamba and S3. AWS Lambda is a serverless computing service that allows to execute code in response to events, without the need to manage servers. Lambda charges only for the time consumed. The use of this computing service allows parallel and almost immediate execution of several functions at once, greatly improving efficiency in this case of fake images masquerading as real photographs or as truthful sources.

It is shown that when a program is run on a local computer it is feasible to perform execution attempts once per core or even on the graphics processing unit for vector computing. With AWS Lambda it is possible to run this program up to a thousand times in parallel and almost immediately without the need for communication between the other programs.

In the case of the experiment, two tools were used almost 1000 images can be generated simultaneously. The equivalence between running 1000 functions and running a single function is in the cost-effectiveness, since Lambda charges are based on the computational capacity used per thousand executions.

AWS Lambda is selected for its cost-effectiveness, among other reasons. AWS Lambda enables the deployment of a software model that includes among other things a generative AI, trained to produce war images that can be perceived as real. On the other hand, S3 is an AWS cloud storage service that offers scalability, data availability, security and performance. Its acronym stands for Simple Storage Service.

To minimize costs, once S3 images are downloaded, temporary files are deleted, except for the preloaded Stable Diffusion file. This serverless architecture creates thousands of fake war images in less than two minutes. It is worth explaining that Stable Diffusion is an artificial intelligence specialized in creating fake images. It works based on textual descriptions. It is part of a family of diffusion models such as machine learning. This AI has been used for artistic purposes.

S3 is like Google Drive, where you can deposit sentences. While Stable Diffusion has been utilized for artistic purposes, the storage component used in this experiment, AWS S3, functions similarly to cloud storage services like Google Drive, allowing for the storage and retrieval of data, such as the text prompts used for image generation. For example, the one executed in this experiment “generate me the images”. Then, under the command of that execution, the generated and deposited images are passed to the Lambda function we defined before, which applies the LUT color patterns to them (those patterns, as we defined before, are the ones that make them look more realistic, which makes it complicated to find out their authenticity with artificial intelligence detection tools).

Figure 1: War image generated, Image obtained from the image bank using the proposed algorithm.

For this experiment, an AI trained exclusively with real photographs of cities in Cyprus and Greece was used. From this training, fake images were generated to which 20 different types of LUTs were applied, completing the production of each batch in 20 seconds. Thanks to the definition of specific thematic patterns, the generated images depicted war scenes, such as smoke plumes, burning buildings or emblematic ruins. This thematic description proved crucial to ensure the accuracy of the AI model in creating the scenes. The procedure is repeated cyclically to produce new images from the established patterns.

When analysing a photographic or digitally generated model, certain concepts must be considered to analyse its possible veracity or falsity. One of the most common methods is to imitate the resolutions of authentic photographs. A common method for generating false images involves taking an existing photograph, reducing its resolution, and then rescaling it. This process alters the image quality (either degrading or artificially enhancing it) to mimic the appearance of a photograph taken with non-professional equipment by an amateur. These basic concepts are explained for application

to counterfeit detection in the final Generative AI model. The ability of an optical system to distinguish between two points close to each other is defined as the optical resolution, which is affected by several factors including the wavelength and the quality of the lenses of the system itself. In more detail:

Lenses: The rays emitted by the object are collected by the essential elements in optics and shaped into image space. A biological example of this type of element would be the crystalline (lens of the eye), which is responsible for collecting the light from the closest elements.

Aperture and diffraction: Depth of field and diffraction (deviation of a wave as it passes through certain obstacles) are affected by the aperture of the lens and are complementary. Thus, a very small aperture can cause diffraction, which reduces optical resolution, while a very large aperture can reduce depth of field, affecting sharpness in certain areas of the image.

Wavelength of light: Optical resolution also depends on the wavelength it receives. Finer details can be resolved by shorter-wavelength light (blue light) than by longer-wavelength light (red light).

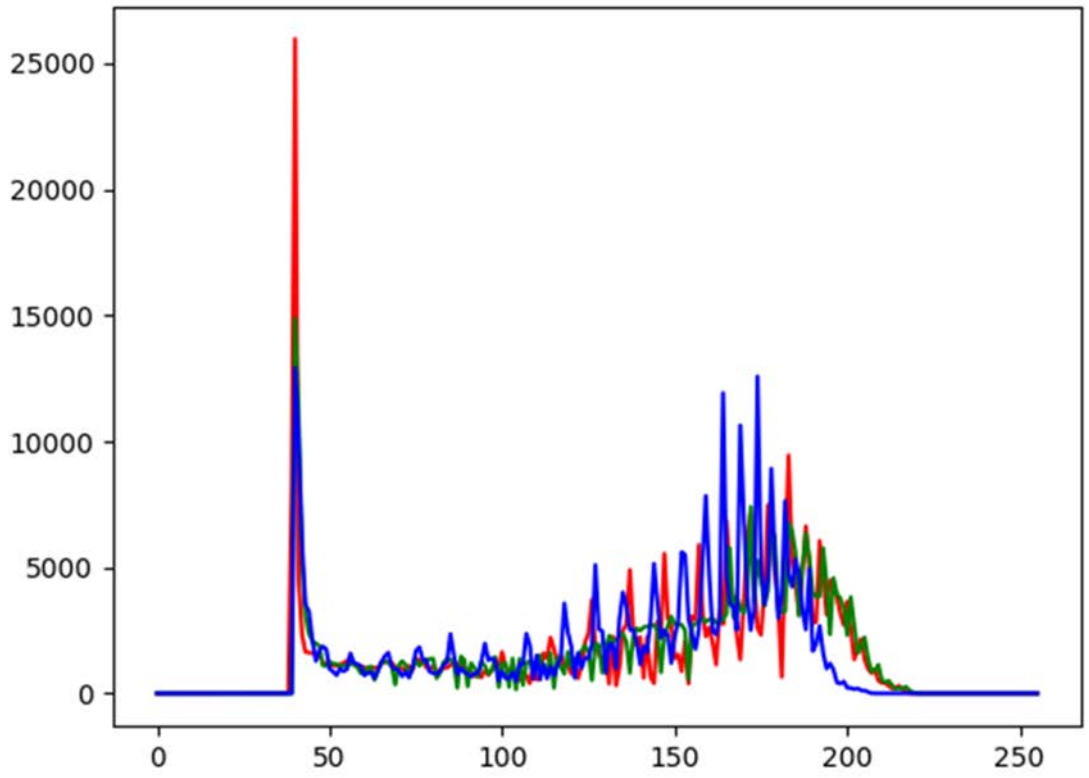

Figure 2: Example of a histogram of a fake war image, graph generated with source code.

These factors are essential in the realization of photographs, since a failure in these elements can result in an incorrect resolution of the photograph, with appearing strange elements (artifacts) in the image. It is here where we find a great similarity with generative artificial intelligences, since these artifacts present in the image can be imitated after a correct description of the requirements or, in the same way, circumvented. This consists of provoking a "misuse" by knowing the possible errors that a photograph may contain with the aim of passing it off as real. People tend to doubt photographs that are "perfect". A parallel is often made between "perfect" and digitally retouched. Ignoring some of these techniques often leads to difficult-to-predict results in Generative AI.

Color is perceived differently in optical and digital media. Optically[3] color perception

[3] Hu, Y., Yang, D., Ma, D., Qi, C., & Huang, S. Structural Color-Based Smart Liquid Windows Address the Tradeoff Between High Optical Transparency and Brilliant Color. Advanced Functional Materials, 2023.

involves elements like wavelength and color temperature. In digital media, however, color is represented using models like the RGB (Red, Green, Blue) or HSV (Hue, Saturation, Value) scales, considering values within those systems and potentially display characteristics like luminance. These scales are different in shape and reference axes. The RGB scale has an ellipse shape and takes into account the coordinates red, green and blue, while the HSV scale has the same shape but considers other coordinates, in this case hue, saturation and color defined as a value.

After creating these images, a thorough analysis of the color histograms corresponding to the images most likely to be passed off as real photographs is essential. These histograms provide highly relevant clues regarding the distribution and intensity of the applied colors, allowing us to extract more color patterns and enhance our generative AI. This, in turn, fosters the creation of a fake image detection system (especially for war-themed images) and facilitates the creation of other automated tools that can recognize AI-created photographs in a more sophisticated way in the future.

Camera optics have several limitations and are based on a series of physical parameters that can be imitated by artificial intelligence, including chromaticity deterioration due to exposure and contrast in photographs, and loss of photographic resolution.

Using the serverless infrastructure of AWS Lambda, S3, and Stable Diffusion enables the creation of fake war images, and the more training is done, the more efficiently generated photographs will be generated. This in turn provides a necessary tool for the development and analysis of advanced image manipulation techniques. In addition to fostering image creation, this will also pave the way for future research into fake news detection and understanding media manipulation in the digital age.

Despite these efforts, distributed computing also presents several challenges. Design and management complexity is significantly greater than in centralized systems. Coordinating and synchronizing multiple nodes can be complicated, and the risk of data consistency and communication issues increases with geographic distribution. Security is also a major concern, as data and processes are distributed across different locations, making it more difficult to protect the integrity and confidentiality of information. Furthermore, fault handling and error recovery in distributed systems require advanced strategies that can

be difficult to implement and maintain.

In the context of AI imaging, distributed computing is used to implement serverless computing solutions. This approach allows developers to focus on the imaging logic without worrying about managing the underlying infrastructure, which is provided by the vendor as a service that simply works. With serverless computing, AI functions can be deployed in the cloud and executed automatically in response to events, such as imaging requests.

Conclusions and results

Since generative AI arrived on social media, it has not been without debate and controversy. AI is the set of tasks performed by computers that would traditionally have required human intelligence[4]. It has been used as a creative medium and as a tool in the medical field (for example, for the detection of various cancers).

Furthermore, within the technological realm, AI applications range "from data analysis and pattern identification to understand complex phenomena to vehicle driving or the generation of visual, textual, and audio content"[5]. However, this same capability now positions AI as a potential weapon in the age of disinformation.

By examining the created images and their color histograms, we gain numerous insights into the impact these images could have if published on television or on a social network like X/Twitter. The first thing to consider regarding the results is that several tools that could currently create images were considered, but Amazon Web Service was chosen. In other words, there was evidence and awareness about tools that could be used to create fake news with the help of these images, which entails an assessment of the ethical conflicts this tool poses. The images created in this study seek to imitate real photographs based on imitating current real-world conflicts, applying different LUTs that contribute to gaining insights into how an image can appear more authentic to the press, social media, and the public. This exploration also involves examining the social, political,

[4] Boulanin Vincent, et al. “Artificial intelligence, strategic stability and nuclear risk”. 2020.

[5] Álvarez-Verdugo, Milagros, “la inteligencia artificial en perspectiva comparada” Revista del Instituto Español de Estudios Estratégicos, n.º 224, pp. 183-215, (2024)

and economic consequences that could arise if this technology becomes accessible, and the public becomes aware of it.

Extremely advanced computing, such as that demonstrated in the experiment, poses a danger in several ways, including those for propaganda purposes and as a weapon against political or cultural rivals. According to Aníbal Monasterio, while AI will transform communication, it increases vulnerabilities. He emphasizes that information quality and integrity—meaning the information is not corrupted, is protected from unauthorized access (privacy), and has clear ownership—are fundamental to security and social values. And by information quality and integrity, we mean not only ensuring that the information is not degraded or corrupted (...) but also ensuring that it is protected and ensured that this information is not accessed without consent (privacy) and that its owner is clearly identified"[6].

The ease with which fake images can be generated and distributed using advanced technologies places a great responsibility on developers and users of social media platforms. Ethical regulations governing the use and distribution of generative content are needed to prevent information manipulation.

This has a multi-pronged impact: the generation of fake images can have significant consequences in social and political contexts, influencing public perception and potentially altering the outcomes of real-life conflicts. It would be interesting to propose and then develop, effective verification methods to ensure the integrity of content shared on media outlets and digital platforms.

To prevent this, public education and awareness are needed to identify fake news, especially those originating from visual sources. Education can act as a counterweight to the rise of fake images, equipping individuals with critical skills to discern the veracity of audiovisual content.

Finally, innovation in fake news detection is worth highlighting: the development of technologies for the automated and efficient detection of fake news is vital to countering

[6] Monasterio Astobiza, Aníbal, "Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos." Dilemata, (24), 185–217, 2017

the spread of disinformation. The integration of serverless systems for rapid analysis and processing of large volumes of images can be a valuable tool in the fight against media manipulation.

*Ms. Estíbaliz García Huete, PhD student, Faculty of Information Science, UCM**

Dr. Sara Ignacio Cerrato, PhD in Optics, Optometry and Vision, UCM

Dr. David Pacios Izquierdo, Assistant Professor, Faculty of Computer Science, UCM

Dr. José Luis Vázquez Poletti, Associate Professor, Faculty of Computer Science, UCM

Dr. Mª José Pérez Serrano, Associate Professor, Faculty of Information Science, UCM

Dr. Andrea Donofrio, Associate Professor, Faculty of Information Science, UCM