A COMPARATIVE REVIEW OF AI-GENERATED IMAGE DETECTION ACROSS SOCIAL MEDIA PLATFORMS

Anjuman Ara¹, Md Sajadul Alam², Kamrujjaman³ Afia Farjana Mifa⁴

¹Management Information Systems, College of Business, Beaumont, Texas, USA. https://orcid.org/0009-0002-1704-8388

²Computer Science and Engineering, Department of Computer Science, American International University-Bangladesh, Bangladesh. https://orcid.org/0009-0001-8014-2038

³Computer Science and Engineering, Department of Computer Science and Engineering, North South University, Bangladesh. https://orcid.org/0009-0004-4696-921X

⁴Computer Science and Engineering, Department of Computer Science, American International University-Bangladesh, Bangladesh. https://orcid.org/0009-0001-5827-152X

Abstract
The proliferation of images generated by artificial intelligence (AI) has significantly impacted the digital landscape, especially on social media platforms where the distinction between natural and synthetic content is increasingly blurred. This study embarks on a comparative review of the strategies used by major social media platforms—Facebook/Instagram, Twitter, TikTok, and YouTube—to detect AI-generated images. Employing a comprehensive methodology that includes a systematic review of academic literature, analysis of platform policies, and expert interviews, this research assesses the effectiveness of various detection methods, ranging from sophisticated AI tools to user reporting mechanisms. The findings reveal diverse approaches: Facebook and Instagram utilise a blend of AI detection and human moderation; Twitter integrates machine learning algorithms with user reports; TikTok emphasises AI tools within moderation workflows and educational initiatives; and YouTube relies on its Content ID system alongside AI analysis. The study highlights the critical role of effective detection systems in maintaining content authenticity and user trust, underscoring the importance of balancing automated detection with human oversight. The ongoing development and refinement of these technologies, alongside collaborative efforts and evolving regulatory frameworks, are identified as essential for ensuring a trustworthy digital environment. This research contributes to the discourse on digital integrity, offering insights into the complexities of safeguarding social media ecosystems against the challenges posed by AI-generated content.

Keywords: AI-generated image detection, Social media content authenticity, Deepfake technology, Content moderation strategies, Digital trust and integrity
Introduction
The digital landscape has been significantly transformed by the rise of artificial intelligence (AI)-generated images have become increasingly prevalent in online media (Tariq et al., 2020). Social media platforms are at the forefront of this transformation, serving as arenas where the authenticity of visual content is constantly tested against the proliferation of synthetic media (Bharati et al., 2016; Hsu et al., 2020). According to Karras et al. (2017), the sophistication of AI techniques, especially those employing Generative Adversarial Networks (GANs), has advanced to a point where the line between genuine and fabricated imagery is often indiscernible. This obscurity poses a substantial challenge to average users and the algorithms designed to detect such content (Zampoglou et al., 2016). As these platforms grapple with the implications of this technological evolution, the need for robust detection mechanisms becomes increasingly critical (Hashmi et al., 2013; Shrivastava et al., 2017). The integrity of these social media ecosystems and the trust users place in them hinges on the ability to discern and authenticate the origins of the content they engage with daily (Shullani et al., 2017).

In response to this emergent challenge, social media giants have begun deploying various strategies to detect AI-generated images and mitigate their potential impacts (Shu et al., 2017). This article examines and contrasts the detection methods currently in use across various platforms. By surveying the landscape of existing technologies, from cutting-edge algorithmic solutions to community-based reporting systems, this analysis aims to shed light on the current state of AI-generated image detection (Parikh & Atrey, 2018; Shu et al., 2017; Y. Wang et al., 2018). The detection of AI-generated content has become a dynamic field, with continuous developments driven by the escalating sophistication of image-generation technologies (McCloskey & Albright, 2019). Platforms are in an ongoing technological arms race, striving to outpace the capabilities of AI generators with more advanced and precise detection algorithms (Singh & Sharma, 2021). This back-and-forth has significant implications for the future of digital content curation and the role of AI in shaping the trustworthiness of shared media (Salim et al., 2022; Sharma et al., 2022).

The importance of understanding and improving AI-generated image detection extends beyond the technical realm; it is a matter that affects the very foundation of how information is perceived and trusted online. With the vast number of users relying on social media for news, personal interactions, and business, the authenticity of visual content has never been more critical. Reliable detection methods are essential to counter the dissemination of deepfakes and other forms of synthetic media that can erode the credibility of online platforms (Elaskily et al., 2021). As AI technology continues to evolve, so must the strategies to combat its misuse. This includes the development of more advanced detection algorithms and the fostering of greater awareness among users about the nature of AI-generated content (Parikh & Atrey, 2018). Ensuring the veracity of shared information in the digital age is a complex, multifaceted endeavour requiring cooperation between technology developers, platform operators, and users (Gaikwad & Hoeber, 2019; Singh & Sharma, 2021). Within this context, this article conducts its comparative analysis, aiming to contribute to the ongoing discussion about maintaining content authenticity in an era increasingly defined by AI.

Background
Artificial intelligence has introduced a groundbreaking method for creating images through algorithms known as Generative Adversarial Networks (GANs) (Salimans et al., 2016). These sophisticated networks consist of a generator that creates images and a discriminator that evaluates their authenticity. Together, they engage in a continuous feedback loop, allowing the generation of images that closely mirror the complexity and detail of real-world visuals (Karras et al., 2017; T.-C. Wang et al., 2018). The use of GANs extends across various domains, including but not limited to
enhancing visual content for films and crafting intricate and lifelike textures for video games (McCloskey & Albright, 2019). Such technology not only showcases the creative potential of AI but also exemplifies the blurring of lines between artificial creations and actual photographic content. The fidelity of these images has progressed to such an extent that it often requires more than a cursory glance to differentiate between an AI-generated image and a genuine photograph, a testament to the rapid advancements in AI capabilities (Guarnera et al., 2020; Hsu et al., 2020). As GANs continue to evolve and become more accessible, their applications are likely to expand further, permeating more sectors and presenting new challenges and opportunities within digital content creation.

The verisimilitude of AI-generated images has introduced considerable complexity to the issue of content authenticity on social media platforms. This evolving technology enables the creation of deepfakes, which are alarmingly convincing counterfeit videos or images (Jeon et al., 2020; Jeon et al., 2020). Such deepfakes can potentially impersonate public figures, fabricate scenarios, or sway public sentiment, thus posing a severe threat to the integrity of information circulated online. The implications of this technological misuse are profound, as they undermine users' trust in digital content. As a result, the distinction between authentic and AI-generated content has become an increasingly common challenge for social media users, leading to a pressing need for reliable verification methods. The uncertainty surrounding the authenticity of online content necessitates a vigilant approach to media consumption and a heightened awareness of the capabilities of AI in image generation (Neves et al., 2020; Shrivastava et al., 2017). With the potential of such technologies to influence social, political, and personal realms, the detection and management of AI-generated content has become a critical concern for maintaining the credibility of digital platforms.

Building on the work of Zhu (2019) and the field defined by pioneers such as Li et al. (2007), the study advances the domain of AI-generated image detection by proposing an interpretable and less computationally intensive methodology. Zhu's approach diverges from the conventional reliance on deep learning and CNNs by employing a two-layer Saab transform model to analyse image patches centred on facial landmarks. This technique mitigates the opacity that typically characterises CNN-based methods, offering a window into the decision-making process that underpins the classification of images as real or fake (Zhu, 2019). The process begins with extracting 68 facial landmarks from real and fake training images. These landmarks are focal points for extracting 32x32 pixel patches, which are then analysed by the Saab transform model to determine the image's authenticity. The process concludes with a Support Vector Machine (SVM) classifier, synthesising the data to render a final verdict on the image's authenticity. This method's transparency not only provides clear insights into its analytic process but also aligns with the growing demand for understandable AI within the realm of digital content management.

Figure 1 illustrates this innovative process, showcasing the flow from the initial image input through the facial landmark extraction, patch analysis, and culminating in the SVM classification. By training separate models for each landmark, Zhu's approach capitalizes on the granularity of facial features, a detail often lost in broader CNN analyses. This methodology's potential to achieve accuracy on par with more complex systems, without sacrificing interpretability, is particularly valuable in the context of social media, where the provenance of an image can have significant implications for public perception and discourse. Incorporating Zhu's (2019) model into the detection frameworks of social media platforms could vastly enhance their ability to discern genuine content from AI-generated forgeries. As these platforms continue to grapple with the deluge of synthetic media, methodologies like Zhu's provide a beacon for developing detection systems that are both effective and user-friendly. This advancement in technology paves the way for a future where digital content
can be consumed with confidence, and the authenticity of media is preserved in the face of increasingly sophisticated AI-generated images (See Figure 1).

Figure 1: AI Generated Image Detection process

Source: Zhu (2019)

To tackle the complexities presented by AI-generated content, the tech industry has rallied to develop an array of detection technologies (Sheng et al., 2018). At the forefront are deep learning models, renowned for their proficiency in pattern recognition, which have been fine-tuned to identify the subtlest of anomalies characteristic of fabricated images. These sophisticated models scrutinize for peculiarities in elements such as texture, lighting, and edge delineation—attributes that typically betray an image's synthetic origins and may elude the human eye's detection (Tahaoglu et al., 2022; Tanaka et al., 2021; Tyagi & Yadav, 2022). In addition to visual analysis, some strategies delve into the digital DNA of images by examining their metadata or tracing the origins of their distribution (Wu et al., 2022). Others have homed in on the distinctive digital 'fingerprints' that generative processes imprint on images. Yet, despite the progress made, the battle to discern AI-generated images is in constant flux. The creation and detection techniques are locked in a perpetual cycle of one-upmanship: as generators become more adept at mimicking reality, detectors must correspondingly escalate their capabilities to unmask these ever-more-convincing digital facades (Zhang et al., 2023). This ongoing contest not only fuels technological advancement but also raises the stakes in ensuring the integrity of shared media content.

The relentless advancement in AI technology propels the task of preserving content authenticity into an ever-evolving challenge (Tyagi & Yadav, 2022). Social media platforms are finding themselves at the crux of this issue, tasked with the responsibility of safeguarding user trust and the integrity of the content shared within their domains. To achieve this, platforms are compelled to employ state-of-the-art detection algorithms that can keep up with the rapid pace of AI-generated image creation. However, technology alone may not suffice (Niu et al., 2021; Zhou et al., 2018). There is a growing recognition of the need for transparency in the mechanisms of detection and moderation, as well as an emphasis on user education. Users equipped with knowledge about the nature of AI-generated content and the means to identify it can serve as an invaluable line of defence against the spread of inauthentic content (Sun et al., 2022; Tahaoglu et al., 2022). As such, the responsibility of platforms extends beyond the technical to encompass the fostering of digital literacy, ensuring that users are well-informed participants in the digital ecosystem. This dual approach, combining technological solutions with informed user engagement, is becoming increasingly essential to navigate the
intricacies of digital media and to maintain the credibility that is fundamental to the social media experience.

Methodology
The methodology underpinning this study involved a comprehensive and systematic review designed to evaluate the detection methods for AI-generated images across several prominent social media platforms. The review commenced with a meticulous search of academic databases and platform-specific documentation to gather relevant literature and policy statements concerning the deployment of AI detection tools and moderation strategies. A selection criterion was rigorously applied to ensure the inclusion of studies that specifically addressed AI-generated content detection and user engagement in content moderation processes. Data collection was augmented through expert interviews to provide qualitative insights into the operational challenges and effectiveness of each platform’s detection methods. Following data synthesis, a comparative analysis was conducted, assessing the platforms’ reliance on AI tools, the role of human moderators, user involvement in reporting suspicious content, and the impact of these combined efforts on maintaining content integrity. The evaluation culminated in the construction of a summarizing table (Table 1) that provides an at-a-glance comparison of the various strategies, their effectiveness, and the implications for users and content creators. This methodical approach facilitated a nuanced understanding of each platform’s tactics in managing the ever-evolving challenge of AI-generated synthetic media.

Findings
Findings from the systematic review of AI-generated image detection across various social media platforms reveal distinct approaches employed by each platform to tackle the challenges posed by synthetic media.

Facebook/Instagram
On the platforms of Facebook and Instagram, a hybrid approach has been adopted to ensure the authenticity of content, where sophisticated AI tools work in tandem with human moderation teams. The AI employed on these platforms is equipped with advanced pattern recognition and anomaly detection capabilities, designed to meticulously scan and identify potential AI-generated images that could breach the platforms’ integrity. When such images are detected, they are flagged for further inspection, which triggers the intervention of human moderators. This second layer of defense is where the nuances of content are evaluated, allowing for the discernment that AI alone may not possess. Human moderators examine the flagged content with a critical eye, considering context, cultural references, and subtleties that the AI may overlook. This balanced methodology is crucial to the process, as it seeks to harness the speed and scalability of AI while ensuring that the accuracy and fairness of content moderation are upheld by human insight. This symbiotic relationship between AI and human judgment is essential in maintaining a seamless user experience, preserving trust, and safeguarding the platforms from the infiltration of deceptive content. It epitomizes the platforms’ commitment to maintaining a genuine space for user interaction, one where efficiency in content moderation does not compromise the thoroughness required in the era of sophisticated digital content creation.

Twitter
Twitter has harnessed the power of machine learning algorithms to create an automated defense against the proliferation of AI-generated content on its platform. These algorithms, steeped in extensive training from expansive datasets, are fine-tuned to detect the faint but telltale signs that characterize synthetic media. The nuanced detection process involves sifting through the digital noise to pinpoint irregularities that may suggest an image’s inauthenticity. Beyond the realm of
algorithmic oversight, Twitter also taps into the collective vigilance of its user base through a user-reporting mechanism. This feature democratizes the process of content moderation, allowing users to act as sentinels who can flag content that raises suspicion. Such a participatory approach not only extends the reach of Twitter's content policing but also fosters a sense of community responsibility. Together, the machine precision of algorithmic flagging and the human intuition of user reports create a layered shield against the subtle infiltration of AI-generated images. This strategy reflects Twitter's acknowledgment of the complexity of content verification in the digital age and its commitment to leveraging both technological and human resources to maintain the authenticity of shared content.

**TikTok**

TikTok's approach to safeguarding its platform against the encroachment of AI-generated content involves a seamless integration of AI detection tools within its content moderation workflows. These tools are not merely passive filters but active scanners that meticulously analyze each piece of uploaded content, probing for indicators of artificial genesis. They scrutinize visual cues that might betray the handiwork of generative algorithms and examine metadata that could reveal traces of digital manipulation. Beyond the deployment of these technological sentinels, TikTok recognizes the power of an informed community. To this end, the platform has embarked on a mission to educate its users, developing initiatives designed to illuminate the hallmarks of AI-generated content. Through tutorials, guidelines, and interactive features, TikTok empowers its users to become active participants in the moderation process. By fostering an environment where users are not only alert to the potential of artificial content but also equipped to recognize its subtleties, TikTok enhances its defenses against the dissemination of synthetic media. This educational strategy is pivotal, as it cultivates a user base that is vigilant, knowledgeable, and engaged in the collective endeavor to maintain the authenticity of the content ecosystem.

**YouTube**

YouTube's Content ID system stands as a testament to the platform's commitment to intellectual property rights and the authenticity of its content, harnessing advanced AI to scrutinize videos at the point of upload. This AI is not simply a tool for detecting copyright infringement; it has evolved to become a sentinel against AI-generated videos, distinguishing between genuine creations and those that may have been artificially fabricated. By analyzing the myriad of visual and audio signals within each video, the AI delves into patterns that human eyes or ears might miss, searching for discrepancies indicative of synthetic production. While this technological prowess is commendable, it brings with it a significant responsibility towards content creators whose livelihoods often hinge on the platform. The AI’s discernment is crucial, as inaccuracies can lead to false positives, resulting in the demonetization or unwarranted removal of videos, disrupting the creators’ revenue streams and potentially stifling creative expression. The precision of YouTube’s AI system is, therefore, of paramount importance, as it navigates the delicate balance between safeguarding against synthetic media and upholding the rights and revenues of genuine content creators. This balance is a cornerstone of YouTube’s platform, ensuring that while it remains a bastion against digital counterfeits, it also continues to be a space where creators can flourish without fear of undue penalization.

**Comparative Analysis**

The comparative analysis of AI-generated image detection strategies across major social media platforms demonstrates a spectrum of effectiveness influenced by the complexity and training quality of AI algorithms. On platforms like Facebook and Instagram, pattern recognition and anomaly detection are paramount, with human moderation providing essential oversight, particularly for content flagged by AI, thus ensuring a balance between technological efficiency and the nuances of
human judgment. Twitter's model leans heavily on machine learning algorithms for initial flagging, augmented by a user-reporting system that, while empowering users to partake in content moderation, introduces the potential for bias and error. TikTok's approach is notable for embedding AI detection tools directly within its content moderation workflow, complemented by educational initiatives aimed at enhancing user discernment regarding AI-generated content. YouTube's Content ID system represents a dual focus on copyright protection and the detection of synthetic media, relying on AI for initial analysis and human moderators for final adjudication, a process that directly impacts content monetization and underscores the need for accuracy in the AI's decision-making process. Across these platforms, the interplay between automated AI tools, human moderation, and user engagement forms a multi-layered defense against the incursion of AI-generated content, each with its own strengths and challenges in the face of scalable content management and the continuous evolution of generative AI techniques (See Table 1).

Table 1: overview of the different strategies employed by each platform.

<table>
<thead>
<tr>
<th>Platform</th>
<th>AI Detection</th>
<th>Human Moderation</th>
<th>User Involvement</th>
<th>Impact on Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook/Instagram</td>
<td>Pattern recognition and anomaly detection</td>
<td>Critical for reviewing AI-flagged content</td>
<td>Limited to reporting suspicious content</td>
<td>Balances efficiency with oversight</td>
</tr>
<tr>
<td>Twitter</td>
<td>Machine learning algorithms for flagging</td>
<td>Secondary to AI, with user-reporting as backup</td>
<td>User-reporting mechanisms for flagging</td>
<td>Empowers users, but susceptible to bias</td>
</tr>
<tr>
<td>TikTok</td>
<td>AI detection tools in content moderation workflows</td>
<td>Part of the workflow, but with emphasis on AI tools</td>
<td>Educational initiatives to inform users</td>
<td>Raises awareness, fosters discerning viewers</td>
</tr>
<tr>
<td>YouTube</td>
<td>Content ID system and AI for pattern analysis</td>
<td>Essential for appeals and complex decisions</td>
<td>Dependent on users for flagging and feedback</td>
<td>Can affect monetization due to false positives</td>
</tr>
</tbody>
</table>

Discussion
The integrity of content on social media platforms is foundational to user trust, a principle that is becoming increasingly significant as AI-generated images become more prevalent (Matern et al., 2019; Selvaraju et al., 2017). Trust in the authenticity of content is not only crucial for user engagement but also for the overall vitality of social media ecosystems (Durall et al., 2019; Matern et al., 2019; Selvaraju et al., 2017). Effective detection methods serve as a bulwark against the spread of (Jalab et al., 2022; Rana et al., 2022; Singh et al., 2020), which carries the potential to skew public discourse and influence socio-political dynamics (He et al., 2018). Platforms that demonstrate the ability to manage the authenticity of their content transparently and reliably are better positioned to sustain and expand their user base. Conversely, the suspicion of manipulated content can erode user trust and diminish platform credibility, potentially leading to reduced engagement (Nguyen et al., 2022). Therefore, the adoption and implementation of advanced detection technologies are imperative, transcending beyond a mere technical pursuit to becoming a strategic component that underpins user retention and the preservation of platform integrity.

However, the introduction of sophisticated detection technologies to identify AI-generated images is fraught with challenges, particularly the risks of false positives and negatives. False positives can result in unwarranted censorship or content removal, adversely affecting creators' visibility and curtailing their freedom of expression—a situation that could lead to revenue loss, diminished audience reach, and reputational damage (Warif et al., 2015). On the flip side, false negatives could permit the circulation of deepfakes or misinformation, thus compromising the reliability of content disseminated on social media platforms. The accuracy of these detection methods is not just a technological imperative but an ethical one, as it significantly impacts the landscape of digital information (Fan et al., 2017). Ensuring precision in detection is therefore critical, as the consequences of failure in this area are far-reaching, affecting not only individual users but the broader societal trust in digital platforms.
The role of human oversight in the content verification process is indispensable. While AI is proficient in managing and analyzing large volumes of content, it inherently lacks the capability for contextual interpretation and cultural nuance (Boulkenafet et al., 2015; Holmes et al., 2016; Martín-Rodríguez et al., 2023). Human moderators are vital for filling these gaps, bringing an understanding of context, sarcasm, and cultural subtleties to the table—nuances that AI systems may misinterpret or overlook entirely. The importance of human intervention in content moderation cannot be overstated, as it ensures that legitimate content is not incorrectly penalized and that the complexities of human expression are accurately considered (Ferrara et al., 2012; Tariq et al., 2020; van den Oord et al., 2016). The interplay between automated systems and human moderation is delicate, with platforms striving to find the right balance between efficiency and precision. The ultimate goal for social media platforms is to foster a collaborative environment where AI and human moderators operate synergistically, combining the scalability of automation with the discernment of human judgment to establish a digital space that is both secure and conducive to genuine expression (Gaikwad & Hoeber, 2019; Sharma et al., 2022; Shu et al., 2017).

Future Directions
The increasing sophistication of AI-generated content heralds a future where the ability to distinguish authentic from synthetic media is paramount, driving an escalating contest between the technologies used to create and detect such content. Social media’s landscape will be inexorably shaped by the progress of AI detection technologies, necessitating persistent innovation and research. This evolution demands an interdisciplinary approach that harnesses cutting-edge machine learning, digital forensics, and cognitive psychology to not only keep pace with but also preempt the next generation of generative AI. Collaborative synergies are vital, with social media entities, technology firms, and academic circles merging their respective data-rich resources, practical insights, and theoretical acumen to pioneer refined detection methodologies. Such partnerships are poised to catalyze significant strides in creating detection models that more closely mirror the intricacies of human-created content. Concurrently, the emergence of rigorous regulatory frameworks and ethical standards plays a crucial role in this landscape, as they must evolve to encapsulate the intricacies of AI’s role in our daily digital interactions. These frameworks and guidelines are tasked with the dual responsibility of mitigating the malicious applications of AI while safeguarding individual liberties and ensuring equitable practices within AI systems. The collective journey towards dependable detection of AI-generated content is complex and layered, intertwining continual technological strides, collaborative dynamism, and stringent oversight. The delicate balance struck in this tripartite interaction will ultimately determine the capacity of social media platforms to curate spaces where authenticity prevails, and user trust in the content they engage with remains unshaken.

Conclusion
The comparative review of AI-generated image detection methods across social media giants like Facebook, Instagram, Twitter, TikTok, and YouTube has unveiled a varied array of strategies each platform employs to mitigate the spread of synthetic content. These platforms leverage AI detection technology for its capacity to efficiently process and analyze vast quantities of data, utilizing pattern recognition and anomaly detection algorithms to identify potential deepfakes. However, the reliance on AI is balanced with human moderators, who are crucial for their ability to provide context-sensitive analysis—interpreting nuances and cultural references that automated systems might miss. Additionally, user participation through reporting mechanisms plays a supportive role, though it carries the inherent risk of introducing bias. The efficacy of these detection systems is pivotal for maintaining content authenticity and securing user trust, as the line between AI-generated and genuine content becomes increasingly blurred. Social media platforms, serving as forums for public
and private expression, must persistently innovate their detection technologies to protect their integrity. The synthesis of automated systems with human oversight is essential for content moderation that is both efficient and discerning. Future efforts must also include collaborative initiatives and the development of regulatory and ethical guidelines to ensure the platforms can provide a reliable and safe digital environment. The continued evolution of AI content and the dedication to ethical innovation are critical for ensuring the online experience remains authentic and secure for users worldwide.

References


