Generative AI Techniques in Image Processing and Emerging Forensic Challenges: A Review

Rashmi Raman[1], Damini Thakur[1], P.N. Ramakrishnan[2]

1. Forensic Professional, Central Forensic Science Laboratory, Directorate of Forensic Science Services, Ministry of Home Affairs, Government of India, Chandigarh -160036

2. Deputy Director & Scientist-D, Central Forensic Science Laboratory, Directorate of Forensic Science Services, Ministry of Home Affairs, Government of India, Chandigarh -160036

Abstract: Image verification and authentication play a very important role in forensic science, since digital images are frequently being misused/exploited with the help of Generative artificial intelligence. AI-based technologies can easily fabricate digital data leading to criminal cases, civil disputes, and intelligence work. Original images are often altered/ morphed /doctored/tampered with advanced machine learning technologies. In legal proceedings, validating the authenticity of the original image in the court of law is very crucial to maintain integrity of evidence. The capabilities of image processing have been greatly improved by recent advancements in artificial intelligence (AI), overcoming earlier limitations. The traditional image editing/morphing methods used by the criminals were easier to decipher by the forensic experts. However, the growing complexity of AI-driven image creation and editing tools both open source and paid tools, presents significant challenges for digital image forensics. The present paper envisages the forensic challenges brought on by AI-generated images, developments in deep learning approaches, such as diffusion models and generative models like GANs, as well as the potential implementations for future research & development of integrated tools to identify image tampering and modification. These technologies, particularly Generative Adversarial Networks (GAN) and diffusion model play a dual role in image forensics, both as a tool for creating highly realistic images such as AI-edited or morphed images, deepfakes, and synthetic media etc. This paper will also help to understand the risks of adversarial attack while describing the new forensic challenges, emphasises the most recent AI methods in image processing, and offers suggestions for future research to address these problems.

Keywords: Artificial Intelligence, deep fakes, GANs, morphed, Nano banana, tampered.

I. INTRODUCTION

1.1 Motivation

Artificial Intelligence (AI) is a comprehensive field that primarily focuses on making machines capable of performing tasks that normally require human intelligence, such as analyzing data, recognizing patterns, or making decisions (1). Generative AI, on the other hand, is a specialized branch within AI that goes beyond analysis and automation. It creates new content like text, images, music, or code by learning patterns from existing data. It employs sophisticated deep learning models to produce a wide array of content, including textual and visual materials, derived from user prompts, thereby progressing beyond merely data-driven functions towards more innovative outputs (2). The rapid proliferation of multimedia content, coupled with the emergence of sophisticated editing instruments, has markedly facilitated the extensive advancement of digital image alteration (3). Techniques such as transformer-based designs, diffusion models, generative adversarial networks (GANs), and convolutional neural networks (CNNs) are designed to check the authentic data from the manipulated content and enabled highly realistic image synthesis, image reversal, restoration, and manipulation (4).

However, digital image forensics faces significant hurdles due to the growing sophistication of generative AI-based image production and manipulation technologies. Because it is now possible to create manipulated visual information with no technical knowledge, from subtle retouching to lifelike deep fakes, manual detection is becoming less and less effective (5). With free and open-source AI tools, anyone can now generate images, edit photos, or even design visuals without needing advanced technical skills. This transition has moved advanced image-processing technology from research settings into everyday use by the public. The growing simplicity of creating and spreading synthetic images poses significant challenges to the authenticity and reliability of visual evidence in fields like forensics, journalism, legal inquiries, national security, and the regulation of social media.

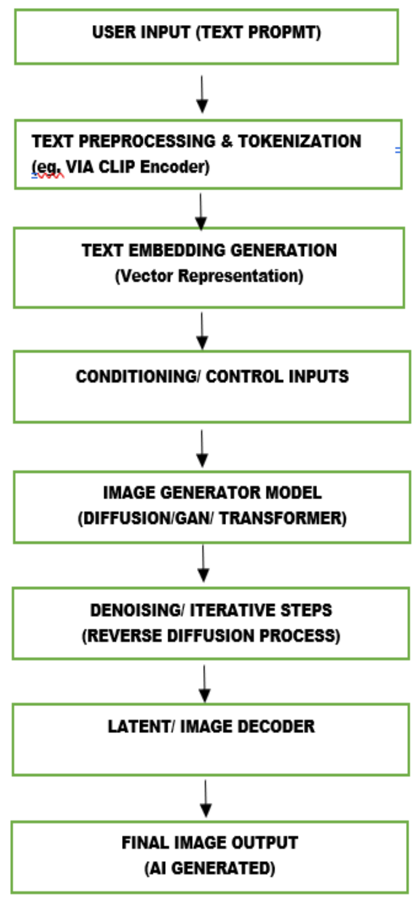
1.2 Scope of Generative AI

Generative AI utilizes Large Language Models (LLMs) which are trained on extensive datasets, to create new content in response to user prompts. It is often considered the next evolution of AI since it goes beyond reusing existing information, enabling the generation of fresh text, images, and other content rather than simply repeating tasks (6). Generative AI applications like ChatGPT, Microsoft Copilot, Google Gemini and Dall-E can produce human-like responses and generate original content based on prompts. These technologies have been developed using several approaches, including GANs, which include components for creating content and another component for evaluating that content for authenticity (7). By doing this, it gives the program feedback or prompt to refine the content, repeating the cycle until the output appears as realistic as possible. Autoencoders strengthen the way generative AI programs reduce the noise patterns while storing and processing data (8).

1.3 Conventional vs new AI image authentication

AI has revolutionized photography and image creation. In the past, studios relied on physical arrangements like props, backdrops, lighting, and expert photographers, demanding considerable time, space, and manual effort to produce varied scenes or intricate effects. Altering backgrounds used to require moving subjects around or relying on green screens, a process that was costly and time-consuming. Now, AI can instantly replace, generate, or enhance backgrounds with the use of Generative AI (9).

Now, Generative AI image processing tools can help users to travel in any landscape in the world without ever leaving their home. Detection of tampered images is very complex as AI can produce a more realistic image reproducing shadows, skin grains, skin texture and even natural lighting conditions (10). These modifications are almost invisible to the naked human eye. Further complexities arise when multiple features like hair, skin texture, grains, marks, moles, clothing etc. are modified by the user by giving a prompt to AI, making the image authentication process in forensics a complex and high-tech challenging task. Even forensic experts need AI-assisted tools and deep learning detection methodologies for analyzing the micro-artifacts for differentiating genuine vs edited images. This requires advanced tools and techniques to detect images processed by AI.



AI Image Generation: Data Flow Diagram (Text-Based Format)

II.EMERGING AI TECHNIQUES IN IMAGE PROCESSING

2.1 Traditional forensic techniques

Image authentication encompasses the process of verifying whether a digital image is authentic, modified, altered, manipulated, and dependable for utilization as evidence in forensic investigations. Altered image identification is essential as they can mislead law enforcement agencies, forensics organizations and court (11). Conventional forensic methodologies for the authentication of images include the analysis of timestamps, the comparison of hash values, the application of watermarking, the utilization of digital signatures, the investigation of EXIF metadata, the identification of tampering, and the validation of sources for digitally altered images. The rapid advancement of artificial intelligence (AI) has significantly improved image generation techniques, making AI-generated images increasingly difficult to distinguish from real photographs. Sophisticated models such as Generative Adversarial Networks (GANs) and diffusion models like Stable Diffusion allow for the creation of highly realistic images with minimal user input (12).

2.2 Stable Diffusion Models

Stable Diffusion Models is a text-to-image generative AI model, uses statistical tools to understand the substance behaviour in a given environment. The diffusion framework models the image generation process as a probabilistic denoising trajectory, wherein structured and high-fidelity images are progressively recovered from stochastic noise distributions under the guidance of textual conditioning (13). With each step, the system uses the text prompt as a guide, refining the image to better match the intended details and meaning. In image processing, the STAPLE diffusion model helps create a consensus segmentation by merging multiple inputs, even when they are not fully consistent. These models aim to explain the process of diffusion, including how it occurs and why it happens. Over time, many diffusion models have been proposed, each approaching the concept in its own way. Notable examples are the Bibendum model, HMM model, k-means clustering model, and random forest classifier.

2.3 Generative Adversarial Network Model

A Generative Adversarial Network (GAN) is a type of machine learning model designed to create data that deviates from the actual, original data (14). It can be used to create manipulated images while simultaneously serving to detect such tampering. The generative component approximates the data distribution, while the discriminator functions as a classifier to separate true data from synthetic outputs.. When both the generator and discriminator reach optimality, the loss function quantifies the divergence between the synthetic dataset and the real-world data distribution.. GANs can be applied to tasks such as image recognition because they can generate realistic samples even when the prompt data contains noise or class labels. This architecture enables the generator and discriminator to be trained simultaneously, helping them adapt more effectively to new datasets compared to traditional generative models (15).

2.4 Wavelet transform method in image processing

The wavelet transform is an effective method in facial recognition, extensively applied for image analysis and the extraction of key features. In contrast to Fourier transforms, which are limited to frequency analysis, wavelet transforms offer simultaneous spatial and frequency localization, enabling effective analysis of localized facial structures. Using wavelet filters, a facial image is decomposed into multiple sub-bands representing coarse and fine features, including approximation and detail coefficients (16). By treating these coefficients as feature vectors, the model can better handle variations in illumination, head position, and expressions during classification. By utilizing multiresolution representations, wavelet-based techniques strengthen the discriminative capabilities of facial recognition systems, facilitating precise and efficient identification under challenging circumstances.

2.5 Image Manipulation Detection and Authentication

This review explores the AI-based methods for detecting morphed, spliced, or otherwise manipulated images It encompasses a range of forensic approaches including pixel-level anomaly detection, feature-based techniques, and deep learning models for image authentication. The study examines the performance of these techniques in identifying diverse image forgeries, with particular attention to accuracy, localization capabilities, and the capacity to separate authentic images from tampered ones.

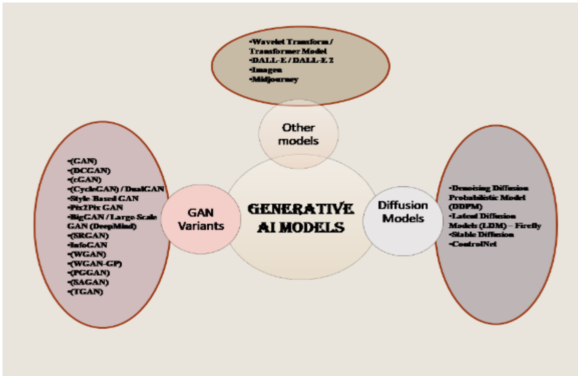


Fig. 1. Hierarchical Layout of Generative AI techniques.

Table 1: Traditional Image Verification vs. AI-Driven Manipulation Detection

Artifacts	Traditional Image Authentication	AI-specific Image Authentication
Visual Analysis	• Fewer inconsistencies • More coherent texture	• Visible Imperfections when zoom/ magnified or focused
Resolution	• Variable Resolution. depending on lighting and lens focus. • Authentic textures and natural details.	• Generate images at fixed resolutions. • Upscaled or resized, or repeated texture patterns and lacks natural variations.
Compression	• Realistic artifacts • Uncompressed	• Digitally processed • Heavily compressed
Anatomical implausibility	• Natural anatomy • Realistic posture	• Anatomical inconsistencies. • Unrealistic posture
Stylistic Artifact	• Subtle realism or natural detail	• Exaggerated detail or unnatural realism
Functional Implausibility	• Spatial coherence with the objects and surrounding elements.	• Design flaws or structural inconsistencies with the objects and surrounding elements.
Forensic Examination	• Image enhancement, authenticity verification, EXIF and metadata analysis	• AI forensic models vulnerable to rapid evolution of manipulation tools (deepfake apps, diffusion models)
Legal/Ethical Risks	• Data privacy breaches	• Misclassification risks (false positives/negatives affecting judicial outcomes, privacy concerns in dataset collection)

III. LITERATURE REVIEW

Numerous studies have explored different methodologies within this area.

Robin Rombach et al. describe the Diffusion model by operating directly on pixel space. The integration of cross-attention layers within the model architecture enhances diffusion models, equipping them to handle general conditioning inputs (e.g., text or bounding boxes) and to achieve high-resolution synthesis in a convolutional framework. The proposed latent diffusion models (LDMs) establish state-of-the-art benchmarks for image inpainting and class-conditional image synthesis and demonstrate strong performance across tasks along with unconditional generation, text-to-image synthesis, and super-resolution, with substantially reduced computational demands compared to pixel-level diffusion models.

Shuxue Ran explores the impact of Generative Adversarial Networks (GANs) in reshaping digital creativity by facilitating the creation of new artistic forms, styles, and transformations using architectures such as DCGAN, WGAN, WGAN-GP, and CGAN.. The study highlights real-world applications through platforms like Stable Diffusion and NovelAI, demonstrating their role in expanding the scope of artistic expression. Alongside these advancements, the paper raises pressing concerns, particularly regarding copyright and ownership of AI-created content, the impact on conventional art sectors, and the place of human creativity in a machine-driven artistic landscape. The conclusion highlights that GANs expand artistic possibilities, yet their integration requires a balanced approach that respects ethical standards, legal frameworks, and cultural values.

Pingyuan Xu et al. summarizes the various algorithms of artificial intelligence and machine learning in image processing, the development process of neural network model, the principle of model and the advantages and disadvantages of different algorithms, and introduces the specific application of image processing technology based on these algorithms in different scientific research fields. This also explains the main applications of facial image recognition. A facial expression recognition system generally has three key components: detecting and normalizing faces, extracting features and analyzing them, and finally classifying and validating the results.

Muhammad Imran & Norah Almusharraf paper further explains Gemini's potential impact on education and its applications in new technologies. It also examines the main obstacles and ethical considerations to ensure Gemini is used effectively and responsibly in the educational field.

Alain Komaty et al. study demonstrates that ChatGPT (GPT-4o) can serve as a strong alternative for Face Presentation Attack Detection (PAD), surpassing the performance of several PAD models, including some commercial systems, in certain scenarios. GPT-4o demonstrates notable consistency, with its few-shot in-context learning performance improving as additional reference examples are supplied. Detailed prompts help the model generate scores more reliably compared to concise prompts, while explanation-oriented prompts slightly boost performance through better interpretability.

Mark Scanlon et al. findings suggest that, although ChatGPT holds considerable promise for digital forensic investigations, the role of human expertise remains indispensable. A key issue highlighted by this research is determining how to effectively balance the advantages of AI with the continued involvement of human expertise.

Savita K Shetty, Ayesha Siddiqa Based on this study, it can be concluded that CNNs are capable of achieving the desired outcomes in deep learning tasks involving image inputs. Nonetheless, convolutional neural networks (CNNs) incur substantial computational expenses owing to their dependence on graphical processing units (GPUs); in the absence of such hardware, their training processes are considerably protracted due to the necessity for extensive training datasets. In numerous instances, this limitation can be mitigated through the utilization of pre-trained models, which can be fine-tuned according to specific requirements.

Shai Farber This investigation systematically assesses the efficacy of artificial intelligence (AI) instruments (ChatGPT-4, Claude, and Gemini) in the forensic examination of crime scene imagery, representing a pivotal advancement toward the creation of customized AI frameworks for forensic utilization. The study entailed an autonomous evaluation of 30 crime scene images by the aforementioned AI tools, with the resultant reports meticulously scrutinized by a panel of 10 forensic specialists. The outcomes indicate a promising capacity for AI to function as a decision support mechanism within forensic science, acting as a swift preliminary screening tool to aid human experts in their thorough analyses. The findings underscore that contemporary AI instruments operate most effectively as adjunctive technologies, augmenting rather than supplanting the expertise of forensic analysis.

Cao, Y et al. study presents an extensive examination of the historical context and recent progressions within the domain of AIGC, placing specific emphasis on both unimodal and multimodal generative models. Furthermore, we engage in a discourse regarding the latest applications of generative AI models, frequently employed methodologies in AIGC, and confront the issues pertaining to trustworthiness and accountability within the discipline. Ultimately, we investigate unresolved challenges and prospective trajectories for AIGC, underscoring potential pathways for innovation and advancement. The principal aim of this survey is to furnish readers with a thorough comprehension of the contemporary developments and forthcoming obstacles in the realm of generative AI. Our evaluation of the overarching framework of AI generation seeks to differentiate present-day generative AI models from their antecedents.

Lei Feng's paper highlights the role of modern AI methods in digital image processing, covering tasks from image conversion and restoration to enhancement, separation, matching, and classification. The authors propose a novel hybrid intelligent algorithm, the BAS-based C algorithm (with BAS likely referring to a bio-inspired or adaptive search strategy), and demonstrate its application across multiple image processing tasks, showing enhanced optimization performance.

Sandeep Singh Sengar paper presents a systematic literature review of the latest developments in generative AI. Specifically, it thoroughly explores key algorithms within the realm of Generative AI, including Diffusion Models, Transformer-based models, Generative Adversarial Networks, Variational Autoencoders, and their advancements tailored to specific applications. The paper thoroughly explores core generative AI algorithms and their tailored advancements, covering Diffusion Models, Transformers, GANs, and VAEs for specialized applications.

Barredo Arrieta et al. offer an extensive review of explainable AI, emphasizing its significance for trust, fairness, accountability, and transparency. It differentiates between transparent models, which are naturally interpretable, and post-hoc explanation approaches for black-box models such as deep neural networks, employing techniques like feature importance, saliency maps, and counterfactual explanations.

IV.FORENSIC CHALLENGES & LIMITATIONS FACED IN AI-GENERATED IMAGES

This section emphasizes the primary challenges associated with the application of AI-based detection techniques to real-world datasets; challenges also arise from compression artifacts, noise, and standard image transformations like cropping and resizing, which can make manipulations harder to detect. Moreover, the review highlights the challenges associated with high-fidelity image manipulations, encompassing adversarial attacks and the development of anti-forensic methods intended to circumvent detection.

The simplicity with which realistic images can be generated raises significant concerns regarding their potential misuse in blackmail, manipulation, and the propagation of misinformation. Artificial intelligence technologies are being leveraged to produce non-consensual sexual imagery, widely termed deepfake pornography (29). By inputting a real person's face and pairing it with explicit reference material, attackers can generate counterfeit pornographic images. Specific AI technologies have been developed to digitally remove clothing from genuine images, resulting in fabricated nude depictions of individuals. This presents a significant obstacle for forensic professionals in the modern technological age to keep up with outdated forensic software.

When an image is captured with a digital camera or smartphone, the sensor records light information such as color and brightness, storing it as a RAW file (.CR2, NEF, ARW, DNG). These files preserve the original image without compression, maintaining full quality, color depth, and metadata like EXIF (Exchangeable Image File Format) and file information (30). Nonetheless, any compression or manipulation of the original images may result in changes to the file format, extension, and metadata.

A major challenge with AI-generated images is the lack of information about the original capturing device, such as camera type, lens, and related details. At times, the source of a captured image cannot be established by forensic software or workstations using EXIF data or metadata alone. In scenarios where original images are shared through social media platforms (e.g., WhatsApp, Snapchat, Instagram, Facebook), metadata regarding the capturing device, camera, and lens is typically unavailable. Therefore the EXIF info and metadata cannot be the only source to prove the manipulation and authenticity of the image.

V.FRAMEWORK, DETECTION AND ADVANCED METHODS

This framework for AI-driven image forensics brings together sophisticated detection techniques and modern methodologies to detect and authenticate altered images. Fundamentally, this framework leverages deep learning architectures, including

CNNs, GANs, and Transformer-based models, to detect subtle manipulations—including deepfakes and morphed images—through analysis of pixel anomalies, feature inconsistencies, and artifacts arising from generative processes (31). Advanced AI-based forensic methods integrate image provenance tracking to trace origin and manipulation history, alongside multi-modal analysis that combines metadata and contextual information for more robust verification. In order to mitigate adversarial attacks and anti-forensic methods, forensic systems utilize robust models with adversarial training and countermeasures, ensuring operational efficacy in real-world contexts. These systems are built to scale for large datasets and support real-time deployment, making them suitable for extensive digital media verification. The overarching objective of this methodology is to establish AI-driven proprietary forensic tools that are not only accurate and efficient but also ethically responsible and legally admissible.

VI.CONCLUSION

The impersonation of fake images and morphed photographs viral on social media platforms has been a major concern nowadays which has sabotaged the Machine Learning systems. The real challenge amongst the forensic fraternity and law enforcement agencies is to distinguish between real image and AI based images. This review highlights some of the important artifacts if carefully visualised can help to distinguish the difference between the two. Image processing has transformed with recently emerging Generative AI techniques such as Diffusion methods – Stable Diffusion, Firefly, Midjourney, DALL-E & Generative Adversarial Networks (GANs) methods such as Style GAN1, Style GAN2, Style GAN3 & EG3D.

When images are shared on platforms like WhatsApp, Instagram, Facebook, or X, important identifiers such as EXIF data and metadata are typically stripped or modified for size reduction and platform optimization. As a result, forensic examiners may find it difficult to determine the true origin, creation tool, or authenticity of the image. In such scenarios advanced analytical techniques such as Noise pattern detection, compression artifact Detection, lightning and pattern inconsistencies other artifacts etc must be done rather than solely depending on EXIF and Metadata of the file. Other morphological characteristics, along with spatial relationships and alignment of facial landmarks helps forensic experts to identify image tampering to a greater extent. While significant progress has been made in the detection of image tampering, however, a deeper understanding and further research are essential to develop more efficient and accessible methods for identifying such manipulations

ACKNOWLEDGMENT

The authors are thankful to Dr. S.K. Jain, Chief Forensic Scientist, Directorate of Forensic Science Services, Ministry of Home Affairs, New Delhi, India and Dr. Sukhminder Kaur, Director, Central Forensic Science Laboratory, Chandigarh for constant support and encouragement for carrying out R&D activities. Also, the author wishes to thank the Scientist of Physics Division, CFSL Chandigarh for the technical know-how and support during the critical stage of interpretation and finalizing the paper.

REFERENCES

[1] Triantafyllou, S. A. (2024, January 23). Artificial intelligence: An overview

[2] Leonardo Banh & Gero Strobel, 2023. "Generative artificial intelligence," Electronic Markets, Springer; IIM University of St. Gallen, vol. 33(1), pages 1-17, December

[3] A. Pandey, P. Parwekar and A. K. Chakraverti, "A Review on Deep Learning Techniques for Image Forgery Detection," 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2022, pp. 890-895, doi: 10.1109/ICCCIS56430.2022.10037746

[4] J. Gui, Z. Sun, Y. Wen, D. Tao, and J. Ye, A Review on Generative Adversarial Networks: Algorithms, Theory, and Applications, arXiv Prepr., vol. 14, no. 8, pp. 1–28, 2020.

[5] K. S. Kaswan, K. Malik, J. S. Dhatterwal, M. S. Naruka and D. Govardhan, "Deepfakes: A Review on Technologies, Applications and Strategies," 2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC), Greater Noida, India, 2023, pp. 292-297, doi: 10.1109/PEEIC59336.2023.10450604.

[6] Hagendorff, T. (2024). Mapping the Ethics of Generative AI: A Comprehensive Scoping Review. Minds and Machines, 34(4). https://doi.org/10.1007/s11023-024-09694-w

[7] Akhtar, Z. B. (2024). Generative artificial intelligence (GAI): From large language models (LLMs) to multimodal applications towards fine tuning of models, implications, investigations. Computing and Artificial Intelligence, 3(1), 1498. https://doi.org/10.59400/cai.v3i1.1498

[8] Chen, S., & Guo, W. (2023). Auto-Encoders in Deep Learning—A Review with New Perspectives. Mathematics, 11(8), 1777. https://doi.org/10.3390/math11081777

[9] Dadkhah, Sajjad & Manaf, Azizah & Sadeghi, Somayeh. (2014). Efficient Image Authentication and Tamper Localization Algorithm Using Active Watermarking. 10.1007/978-3-662-43616-5_5

[10] Chakraborty, Sunen & Dey, Paramita & Chatterjee, Kingshuk. (2023). Digital Image Tampering Detection Using Deep Learning: A Survey. 10.1007/978-981-99-2710-4_17.

[11] Khalil, Hady & Maged, Shady. (2021). Deepfakes Creation and Detection Using Deep Learning. 1-4. 10.1109/MIUCC52538.2021.9447642.

[12] Goyal, H., Wajid, M. S., Wajid, M. A., Khanday, A. M. U. D., Neshat, M., & Gandomi, A. (2025, January 2). State-of-the-art AI-based learning approaches for deepfake generation and detection: Analyzing opportunities, threading through pros, cons, and future prospects

[13] Castillo Camacho, I., & Wang, K. (2021). A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics. Journal of Imaging, 7(4), 69. https://doi.org/10.3390/jimaging7040069

[14] Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014, June 10). Generative adversarial nets.

[15] Marques, B. A. D., Batagelo, H. C., & Gois, J. P. (2023). A review on generative adversarial networks for image generation. Computers & Graphics, 114, 1-13. https://doi.org/10.1016/j.cag.2023.05.010

[16] Abdulazeez, Adnan & Zeebaree, Diyar & Zebari, Gheyath & Mohammed, Idrees & Adeen, Najim. (2020). Journal of Soft Computing and Data Mining The Applications of Discrete Wavelet Transform in Image Processing: A Review. 31-43. 10.30880/jscdm.2020.01.02.004.

[17] A.Rombach, Robin & Blattmann, Andreas & Lorenz, Dominik & Esser, Patrick & Ommer, Bjorn. (2022). High-Resolution Image Synthesis with Latent Diffusion Models. 10674-10685. 10.1109/CVPR52688.2022.01042.

[18] Ran, Shuxue. (2024). Applications and challenges of GAN in AI-powered artistry. Applied and Computational Engineering. 41. 75-79. 10.54254/2755-2721/41/20230713.

[19] Xu, Pingyuan & Wang, Jinyuan & Jiang, Yu & Gong, Xiangbing. (2024). Applications of artificial intelligence and machine learning in image processing. Frontiers in Materials. 11. 10.3389/fmats.2024.1431179.

[20] Imran, Muhammad & Almusharraf, Norah. (2024). Google Gemini as a next generation AI educational tool: a review of emerging educational technology. Smart Learning Environments. 11. 1-8. 10.1186/s40561-024-00310-z.

[21] Komaty, Alain & Otroshi, Hatef & George, Anjith & Marcel, Sébastien. (2025). Exploring ChatGPT for Face Presentation Attack Detection in Zero and Few-Shot in-Context Learning. 1602-1611. 10.1109/WACVW65960.2025.00093.

[22] Scanlon, Mark & Breitinger, Frank & Hargreaves, Christopher & Hilgert, Jan-Niclas & Sheppard, John. (2023). ChatGPT for digital forensic investigation: The good, the bad, and the unknown. Forensic Science International: Digital Investigation. 46. 301609. 10.1016/j.fsidi.2023.301609.

[23] Shetty, Savita & Siddiqa, Ayesha. (2019). Deep Learning Algorithms and Applications in Computer Vision. International Journal of Computer Sciences and Engineering. 7. 195-201. 10.26438/ijcse/v7i7.195201.

[24] Farber S. (2025). AI as a decision support tool in forensic image analysis: A pilot study on integrating large language models into crime scene investigation workflows. Journal of forensic sciences, 70(3), 932–943. https://doi.org/10.1111/1556-4029.70035

[25] Cao, Yihan & Li, Siyu & Liu, Yixin & Yan, Zhiling & Dai, Yutong & Yu, Philip & Sun, Lichao. (2023). A Comprehensive Survey of AI-Generated Content (AIGC): A History of

Generative AI from GAN to ChatGPT. 10.48550/arXiv.2303.04226.

[26] Feng, Lei. (2022). Application Analysis of Artificial Intelligence Algorithms in Image Processing. Mathematical Problems in Engineering. 2022. 1-10. 10.1155/2022/7382938.

[27] Singh Sengar, Sandeep & Hasan, Affan & Kumar, Sanjay & Carroll, Fiona. (2024). Generative Artificial Intelligence: A Systematic Review and Applications. 10.48550/arXiv.2405.11029.

[28] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

[29] Vamsi, Vurimi & Shet, Sukanya & Reddy, Sodum & Rose, Sharon & Shetty, Sona & Sathvika, S & M S, Supriya & Shankar, Sahana. (2022). Deepfake Detection in Digital Media Forensics. Global Transitions Proceedings. 3. 10.1016/j.gltp.2022.04.017.

[30] Mani, R.G., Parthasarathy, R., Eswaran, S., & Honnavalli, P.B. (2022). A Survey on Digital Image Forensics: Metadata and Image forgeries. Workshop on Autonomic Communication.

[31] Kamali, Negar & Nakamura, Karyn & Chatzimparmpas, Angelos & Hullman, Jessica & Groh, Matthew. (2024). How to Distinguish AI-Generated Images from Authentic Photographs. 10.48550/arXiv.2406.08651.