International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Generative Threats in Computer Vision: Dual-Role Gans and Diffusion-Based Defenses for Robust and Trustworthy Models

Mahesh Kumar[1]*, Tanvi Rustagi [2]

[1]Research Scholar, Department of Computer Science and Engineering, World College of Technology and Management, Farukh Nagar, Gurgaon, Haryana, India

Orcid id: 0009-0005-0777-7802

[2]Assistant Professor, Department of Computer Science and Engineering, World College of Technology and Management, Farukh Nagar, Gurgaon, Haryana, India

Orcid id: 0009-0002-9639-0228

Abstract - Generative Artificial Intelligence (GenAI) has revolutionized computer vision with cutting-edge image generation, semantic interpretation, and adaptive visual reasoning capabilities, while also bringing new security, robustness, and trustworthiness concerns. In this review, the twenty five recent studies related to generative threat and diffusion-based defense mechanism in computer vision and intelligent network systems were analyzed in a systematic manner based on PRISMA based literature review methodology. The studies reviewed showed that Generative Adversarial Networks (GANs), diffusion models, transformer models, and large language models are dual-use technologies that can be used to create powerful adversarial attacks and powerful defense frameworks. The analysis identified the shifting nature of adversarial attacks—from perturbations at the pixel level to latent-space attacks, multimodal deepfakes, semantic communication attacks and cyber deception by AI tools. At the same time, diffusion-based purification frameworks, federated defense systems, anomaly detection models, and transformer-based verification mechanisms demonstrated high potential to enhance robustness, semantic consistency, privacy preservation, and real-time resilience. The results also showed that synthetic data generation has a notable positive impact on learning performance for low-data scenarios like military object detection and cyber security applications. The issues of computational complexity, attack transferability, scalability and benchmarking inconsistency, however, have yet to be addressed. The review finds that the hybrid generative defense architectures that combine diffusion models, federated learning, explainable AI, graph neural networks, and adaptive semantic verification mechanisms will become increasingly vital for future trustworthy computer vision systems in order to foster secure, resilient, and interpretable next-generation AI systems.

Keywords: Generative Artificial Intelligence, Generative Adversarial Networks, Diffusion Models, Computer Vision Security, Adversarial Attacks, Adversarial Machine Learning, Deepfake Detection, Trustworthy AI, Robustness, Synthetic Data Generation.

1. INTRODUCTION

Recent advances in Generative Artificial Intelligence (GenAI) have significantly transformed the field of computer vision, enabling machines to generate, manipulate, and interpret visual content with unprecedented realism and efficiency [1]. Advancements in image generation, object detection, medical imaging, autonomous systems, surveillance, and multimedia applications have been spurred by technologies like Generative Adversarial Networks (GANs), diffusion models, variational autoencoders, and transformer-based architectures [2]. These generative models have shown great potential in generating high-quality synthetic images, augmenting data, learning from low data, and in powerful visual reasoning in complex environments [3]. In parallel with these technological advances, however, there have been serious security, reliability, and trustworthiness concerns with modern computer vision systems arising from generative models [4].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

As Generative techniques have improved, highly realistic adversarial examples, deepfakes, synthetic identities and manipulated visual evidence can be created, as well as stealthy perturbations that can trick deep neural networks and human observers[5]. From pixel-level perturbations, attacks have become physically achievable, been transformed to the latent space, concealed perturbations that can preserve identity, and multimodal deceptive attacks for computer vision models[6]. These attacks pose a potential threat to the reliability of applications like autonomous vehicles, biometric authentication, intelligent surveillance, diagnostics in healthcare, military systems, wireless communication infrastructure and edge robotics[7]. GANs and diffusion models are now two-in-one technologies which can be used for creating advanced attacks and can also be used for enhancing the robustness, anomaly detection, adversarial purification, synthetic data augmentation, and trustworthy model training[8].

To cope with these new challenges, different types of defense have been proposed to enhance the robustness and security of computer vision systems. Diffusion-based purification frameworks, adversarial training strategies, latent-space reconstruction methods, and semantic verification systems have demonstrated potential in mitigating adversarial vulnerabilities, as well as federated defense architectures and generative anomaly detection models. Furthermore, as computer vision systems grow in complexity and sophistication, explainable AI, graph neural networks, transformer-based security architectures and privacy-preserving learning frameworks are now being embedded in comprehensive computer vision pipelines to improve transparency, resilience and trustworthiness[10]. While significant advances have been made, current defenses still have significant shortcomings with respect to computational complexity, transferability of attacks, real-time deployment considerations, generalization capacity, scalability, and the absence of standardized frameworks for assessing the robustness of a defense.

In this review paper, we systematically survey 25 recent research contributions that address generative threats in computer vision along with diffusion-based defenses, including those related to adversarial machine learning, deepfakes generation and detection, semantic communication security, federated learning defense systems, autonomous vehicle safety, anomaly detection, wireless intelligent networks, and trustworthy AI governance. The analyses of the reviewed research papers shows how GANs and diffusion models have developed into strong attack models but also good defense models. Using the literature analysis, a structured taxonomy of generative threats, defense paradigms and trustworthy AI mechanisms for computer vision applications is developed.

In addition, this paper points out key research gaps in adversarial robustness, multimodal security, semantic consistency verification, low-data defense learning, computational efficiency, human-centered AI trust, and deployment-time certification. The review also includes a discussion of nascent opportunities from adversarial purification with diffusion, synthetic data generation for secure training, generative reinforcement learning for adaptive defence, and explainable trustworthy AI model frameworks. In summary, this study seeks to equip researchers, practitioners, and policymakers with a comprehensive perspective on both the evolving landscape of generative AI technologies and their impact on computer vision systems' security, fostering the creation of more resilient, interpretable, and trustworthy computer vision AI models.

2. REVIEW METHODOLOGY

2.1 Literature Search Strategy

The aim of this review paper is to perform systematic literature review to retrieve, analyze and synthesize the recent research work on generative threats and diffusion-based defense for computer vision systems. The key areas of the review included Generative Adversarial Networks (GANs), diffusion models, adversarial machine learning, deepfake generation and detection, trustworthy AI, anomaly detection, and strong defense mechanisms in intelligent vision systems. To ensure a wide coverage of interdisciplinary research on computer vision security and generative artificial intelligence, major databases such as Scopus, Web of Science, ScienceDirect, IEEE Xplore, ACM Digital Library, SpringerLink, and Google Scholar were searched.

Relevant studies were retrieved using targeted keywords and search combinations, such as “Generative AI in computer vision,” “GAN adversarial attacks,” “diffusion-based defense,” “deepfake detection,” “adversarial machine learning,” “semantic communication security,” “trustworthy AI,” “synthetic data generation,” “diffusion purification” and “autonomous vehicle security,” “anomaly detection,” and “robust computer vision systems”. Boolean operators (AND, OR and NOT) were used to enhance the accuracy and relevance of search results. Furthermore, methods of forward and backward citations were employed to find citations of influential and highly cited studies related to generative attacks, adversarial robustness, and trustworthy AI frameworks.

In the preliminary search, around 390 research papers were identified from the past five years (2020–2025), in line with the swift evolution of generative AI and computer vision security research.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

2.2 Inclusion and Exclusion Criteria

To ensure reviewed studies were of a high quality, relevant, and technically consistent, specific inclusion and exclusion criteria were put in place. The inclusion criteria included peer-reviewed journal articles, conference papers, survey papers, workshop papers, and high-quality preprints that were relevant to the theme of generative AI applications in computer vision security. In the review, studies pertaining to adversarial attacks, GANs, diffusion models, deepfake systems, adversarial purification, federated defense mechanisms, anomaly detection, semantic communication security, synthetic data augmentation, trustworthy AI governance, and robust autonomous systems were considered.

Studies emphasizing the experimental validation, defense architectures, generative modeling strategies, diffusion-based purification techniques, and transformer-based verification systems, as well as practical applications of computer vision robustness and security were emphasized. Most selected studies were published between 2023 and 2026 to capture the latest developments in generative AI–driven security research.

The studies were not included if they were not related to computer vision, generative AI, adversarial machine learning, or trustworthy AI systems. Papers were excluded for not having been well methodologically developed, not having been sufficiently analyzed experimentally and not being directly related to generative threats and defense mechanisms. To ensure consistency and reliability within the review process, duplicate records, non-English publications, opinion only articles and studies that do not have established evaluation procedures were also excluded.

2.3 Study Selection Process

The process of selection of the studies was carried out in a systematic way and was transparent, reproducible, and systematically screened using the PRISMA 2020 framework. At the identification phase, about 390 items were retrieved from the retrieved academic databases. Eighty-five (85) duplicate records were removed, leaving 305 studies for title and abstract screening.

During the screening phase, studies not related to adversarial attack, generative AI, diffusion-based defenses, trustworthy AI or computer vision security were filtered out. This resulted in the deletion of almost 230 records as they failed to meet the aims of this Review. The other 75 studies were fully reviewed for eligibility.

Each study was assessed at the eligibility stage on methodological quality, experimental validation, relevance to generative threats and defense mechanisms, and contributions to strong and reliable computer vision systems. Only studies that were reproducible, had adequate evaluation metrics, and were directly applicable to adversarial robustness and generative defense research were included in the study. After this evaluation, 25 studies were chosen out of the total for final qualitative synthesis and detailed analysis.

The selected studies were then grouped into thematic areas such as adversarial attack frameworks, diffusion-based purification, deepfake generation and detection, semantic communication security, federated cybersecurity defense, anomaly detection, synthetic data generation, autonomous vehicle safety, trustworthy AI governance, and generative defense architectures. The identified research trends, research limitations, open challenges and future research directions for a robust and trustworthy computer vision system with generative AI were developed based on these thematic categories.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

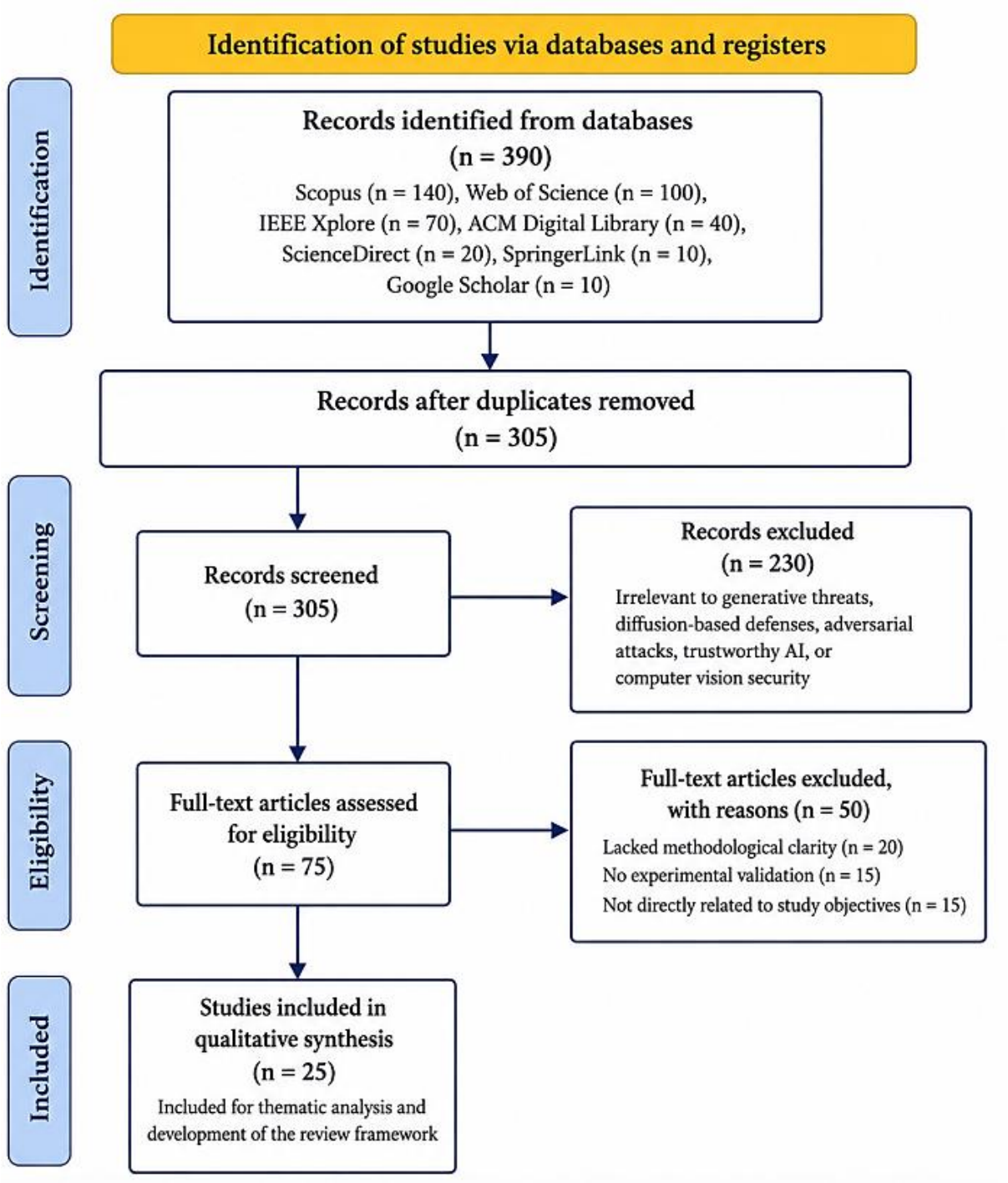

Figure 1. PRISMA Flow Diagram Illustrating the Study Selection Process for Systematic Review

3. Review of Selected Studies

3.1 Adversarial Attacks and Generative Threats in Computer Vision

Recent advances in generative artificial intelligence have significantly increased the sophistication of adversarial attacks against computer vision systems. Adversarial perturbations generated from several of the reviewed works demonstrated that GANs, diffusion models, and transformer-based architectures could produce highly realistic perturbations that could fool deep learning systems without being noticed visually. Guo et al.[11] gave an extensive review of adversarial attack methods, including gradient-based attacks like FGSM and PGD, as well as physically realizable and latent-space attacks on semantic representations in neural networks. Their results indicated the development of adversarial approaches from a trivial level of pixel manipulation to transferable and adaptive attack strategies which can impact on real-world computer vision approaches.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Likewise, Mitra et al. [17] explored the escalating threats of deepfakes and multimodal synthetic media created by combining deepfake models with large language models. The study highlighted that multimodal AI systems can manipulate images, videos, audio, and text to create realistic content, creating the potential for misinformation, impersonation attacks, and digital trust erosion. In adversarial scenarios, Zhang et al.[20] explored vulnerabilities in semantic communication systems, including adversarial inference poisoning, adversarial interference, and distributed inference manipulation in AI-native wireless communication settings.

Kalejaiye et al. [22] studied adversarial machine learning in cybersecurity and classified the adversarial attacks into three categories: evasion attacks, poisoning attacks, and model inference attacks against deep neural networks. The study underscored the increasing significance of strong optimization and explainable AI capabilities to safeguard AI-powered cybersecurity systems. Also, Zhang et al. investigated the propagation of malware in WSNs using a Cellular Automaton–based malware diffusion model, and proposed that an intelligent propagation model can give better prediction and optimizing defense of malware propagation in WSNs.

Table 3.1 Studies on Adversarial Threats and Security Risks

Ref.	Authors	Main Focus	Key Contribution
[11]	Guo et al.	Adversarial attacks in computer vision	Surveyed FGSM, PGD, latent-space and physical attacks
[17]	Mitra et al.	Deepfakes and LLMs	Analyzed multimodal synthetic deception and detection
[20]	Zhang et al.	Semantic communication security	Developed AI-centered threat taxonomy
[22]	Kalejaiye et al.	Adversarial ML in cybersecurity	Examined evasion and poisoning attacks
[35]	Zhang et al.	Malware diffusion in WSNs	Proposed Cellular Automaton malware model

3.2 Diffusion-Based Defense Mechanisms and Robustness Enhancement

The diffusion-based purification and generative reconstruction frameworks are potential defense methods for boosting robustness against adversarial attacks. In the realm of intelligent network services, Du et al.[12] and Du et al.[15] analyzed the dual application of generative AI in network services, showing that diffusion-based defense systems enhanced the reliability of communications and lowered the number of retransmissions in an adversarial setting. They demonstrated in their experiments that AI-driven defense strategies could lead to a decrease in energy usage and increase in network resilience.

Huai et al. [27] introduced R²DShield, a lightweight real-time adversarial defense framework for autonomous mobile platforms used for object detection. The framework combined Bayesian guided perturbation diversification, latent manifold projection and purification mechanisms based on generative adversarial networks to eliminate adversarial perturbations while maintaining the detection accuracy. Experimental evaluation showed that with minimal latency overhead, there were significant improvements in robustness.

Fan et al. [28] proposed the HGDS framework for federated intrusion detection for IOT environments. They used diffusion-based synthetic sampling, hypernetwork grouping and adaptive adversarial defense strategies for enhancing robustness in non-IID and adversarial settings. The study showed significant improvements when it came to F1-score and resistance to poisoning attacks. Fokkinga et al. investigated diffusion generated synthetic data for military object detection in low data volumes [24]. The study showed significant gains in object detection performance by augmenting synthetic images, particularly in low-resource settings, using FLUX and ControlNet-based architectures.

Table 3.2 Diffusion-Based Defenses and Robustness Frameworks

Ref.	Authors	Proposed Method	Major Outcome
[12]	Du et al.	Diffusion-based network defense	Improved energy efficiency and resilience
[15]	Du et al.	AI-driven adaptive defense	Reduced retransmission requirements
[24]	Fokkinga et al.	FLUX-ControlNet synthetic generation	Improved military object detection accuracy

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

[27]	Huai et al.	R²DShield framework	Enhanced adversarial robustness in real time
[28]	Fan et al.	HGDS federated framework	Improved IIoT intrusion detection performance

3.3 Trustworthy AI, Governance, and Ethical Security Frameworks

The studies reviewed had a number of major themes, among which trustworthiness, explainability, fairness, and governance stood out. Huang et al.[13] presented TrustGen, a benchmarking framework for assessing generative foundation models in terms of fairness, privacy, robustness and societal impact. Persistent vulnerabilities in relation to hallucination, misinformation generation, and safety alignment were identified.

Jiang et al. proposed an extensive AI governance framework that focuses on three key areas: Intrinsic Security, Derivative Security, and Social Ethics.[18] One key aspect of the study was the idea that AI governance should be considered a fundamental principle that combines technical soundness and ethical responsibility. Li et al.[21] also explored the trustworthy machine learning by performing the analysis of memorization and suggested a granular long-tail framework with the issues of fairness, robustness and privacy regarding data memorization.

Almarwani et al. [26] presented a human-centric cybersecurity awareness framework that combines the cognitive principles of security with deception analysis using AI. Their empirical results indicated that a crucial factor in protective cybersecurity behaviors towards AI-generated threats is the detection competence. Hao et al. [34] explored how advanced AI systems might impact patent law and innovation, particularly in the context of their potential to redefine the meaning of analogous prior art and the non-obviousness doctrine.

Table 3.3 Trustworthy AI and Governance-Oriented Studies

Ref.	Authors	Research Area	Main Contribution
[13]	Huang et al.	Trustworthy GenAI	Introduced TrustGen benchmarking framework
[18]	Jiang et al.	AI governance	Proposed integrated governance framework
[21]	Li et al.	Trustworthy machine learning	Developed granular memorization framework
[26]	Almarwani et al.	Human-centered cybersecurity	Proposed AI-Cyber-User Awareness Framework
[34]	Hao et al.	AI and patent law	Examined AI impact on analogous prior art

3.4 Generative AI for Autonomous Systems and Intelligent Networks

A few studies were reviewed that studied the role of generative AI to enable intelligent autonomous systems and next generation communication infrastructure. Andreoni et al.[16] have investigated the application of generative AI in autonomous systems such as UAVs, self-driving cars and robotic systems. The study pointed out to applications of predictive analytics, adaptive threat mitigation, anomaly detection, and resilient control systems.

Hu et al. [14] proposed and investigated secure communications based on Generative AI using Space-Air-Ground Integrated Networks (SAGINs). Their survey showed the benefits of GANs, VAEs, diffusion models and large language models for adaptive threat detection, communication optimization, and intelligent intrusion prevention in dynamic cross-domain communication systems.

Zhu et al. [25] studied Wireless Large AI Models (WLAMs) for 6G and beyond wireless communication systems. The study pointed to the synergy between semantic communication, edge computing, intelligent reflecting surfaces, and AI-native communication infrastructures for enhancing the intelligence and adaptable control of communication networks. Zheng et al.[31] also studied contingency planning in autonomous vehicles, which they divided into two types: reactive and proactive paradigms for handling hazards, uncertainties, and semantic anomalies in an autonomous driving system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Table 3.4 Autonomous Systems and Intelligent Communication Studies

Ref.	Authors	Application Area	Key Findings
[14]	Hu et al.	SAGIN security	Applied GAI for adaptive communication security
[16]	Andreoni et al.	Autonomous systems	Enhanced resilience and cybersecurity
[25]	Zhu et al.	WLAMs and 6G	Explored AI-native wireless communication
[31]	Zheng et al.	Autonomous vehicle safety	Proposed hybrid contingency planning framework

3.5 Synthetic Data Generation and Scientific Applications

The use of generative AI in scientific modeling, biomedical research, and anomaly detection also showed promising results. Mo et al.[29] explored strategies for discovering antimicrobial peptides (AMPs) via transformer-based protein models, diffusion models, and reinforcement learning approaches for multi-objective therapeutic optimization.

Poliner et al.[30] introduced a generative modeling approach that is based on graph neural networks, diffusion models, and Bayesian optimization for multiscale material modelling under sparse data conditions. Their method had enhanced the efficiency of the synthetic generation of microstructure and constitutive model for engineering applications.

Noghre et al. [32] proposed a transformer-based spatio-temporal video anomaly detection architecture, called SPARTA, which focused on preserving privacy in anomaly detection. In the field of biological sciences, Wu et al. [33] investigated the applications of generative and self-supervised machine learning, including genomics, RNA analysis, protein modeling, and the generation of therapeutic molecules.

Table 3.5 Synthetic Data and Scientific AI Applications

Ref.	Authors	Domain	Major Contribution
[29]	Mo et al.	Antimicrobial peptide discovery	Applied AI for AMP optimization
[30]	Poliner et al.	Material modeling	Integrated diffusion and Bayesian optimization
[32]	Noghre et al.	Video anomaly detection	Proposed SPARTA transformer framework
[33]	Wu et al.	Biological sciences	Applied generative ML to genomics and proteins

4. FINDINGS AND DISCUSSION

Systematic review of 25 selected studies showed that generative artificial intelligence has created a paradigm shift in the offensive and defensive aspects of computer vision security and intelligent communication systems. Various technologies like Generative Adversarial Networks (GANs), diffusion models, transformer models, and large language models were consistently found to enhance the potential of AI systems for producing realistic synthetic content, semantic manipulations, and adaptive adversarial attacks. At the same time, the same technologies were being more widely used as powerful anti-hacking tools for adversarial purification, anomaly detection, secure communication, synthesis of additional data, and trustworthy deployment of AI.

A key discovery was the swift advances in adversarial attacks in computer vision and AI-enabled communication systems. Previous attacks were mainly gradient attacks like FGSM and PGD; however, recent research identified the shift towards more complex latent space attacks, semantic attacks, multimodal deepfake generation, and physically realizable attacks. The reviewed studies demonstrated that these attacks were successful in achieving transferability, stealth, and adaptability in various object detection systems, autonomous vehicles, semantic communication infrastructure, and cybersecurity applications. The use of deepfakes with large language models compounded the risks of misinformation, synthetic identity theft, and AI-powered deception.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

An important result was related to the effectiveness of defense mechanisms based on diffusion and the reconstruction of the memory through generative processes. Multiple studies showed that diffusion-guided purification techniques could successfully filter out unwanted perturbations, while maintaining semantics and visual quality. Diffusion-based approaches demonstrated greater robustness against adaptive and transferable attacks than traditional adversarial training methods. The real-time defense systems, including R²DShield and federated diffusion-based Intrusion Detection Systems, also highlighted that lightweight generative purification mechanisms can be used to offer robust protection with minimal computational overhead in the edge- and mobile environments.

Another key takeaway from this review is the increasing significance of the generation of synthetic data to enhance the performance of AI in situations of limited data. The diffusion-based synthetic data significantly improved the performance of object detection in military surveillance, cybersecurity intrusion detection and scientific modeling. Research on FLUX-ControlNet frameworks and generative microstructure modeling has validated that synthetic data augmentation did not sacrifice task-specific semantic consistency, and also decreased reliance on costly real-world datasets. The literature also identified some concerns about synthetic bias, unrealistic feature generation, and distributional inconsistencies that could have a negative impact on model generalization and trustworthiness.

A trustworthy AI governance and explainability also appeared as a key theme among the studies reviewed. The importance of incorporating fairness, transparency, accountability, robustness, and privacy preservation into AI security paradigms was highlighted by several researchers. Governance-oriented research revealed that the existing evaluation processes and regulatory mechanisms were fragmented and inadequate to deal with the disruptive generative challenges. Human-centric cybersecurity research also found that knowledge was not enough to fight AI-generated deception, highlighting the need for detection skills, cognitive resistance, and verifiable, explainable systems.

The studies reviewed also revealed that hybrid computer vision security systems that combine diffusion models, federated learning, graph neural networks, reinforcement learning, transformer-based reasoning systems, and explainable AI frameworks would become more prevalent in the future. The hybrid methods presented promising prospects for robust systems, preserving privacy and semantic consistency, and providing adaptive strength in dynamic real-world settings with strong potential for scalability. However, there were a number of important issues not addressed, such as computational complexity, the transferability of attacks to different architectures, the lack of uniformity in benchmarks, limitations in deployment time in real-time systems and the absence of standardized frameworks to certify systems as robust.

5. CONCLUSION

Twenty-five recent studies on computer vision systems' generative threats, adversarial attacks and diffusion-based defenses, trustworthy AI, and intelligent communication security were analyzed systemically in this review. The results indicated that generative AI (GAI) technologies, such as GANs, diffusion models, transformer architectures, and large language models (LLMs), have created a new dual-role paradigm that has enabled powerful attack capabilities and sophisticated defense strategies. The presented research work showed that diffusion-based purification, federated defense, anomaly detection systems, and synthetic data generation greatly enhanced robustness and adaptability, as well as performance in various applications, including autonomous systems, cybersecurity, semantic communication, and low-data object detection. Meanwhile, important problems like computational burden, adversarial transferability, scalability issues, benchmarking inconsistencies, and semantic attack vulnerabilities are yet to be solved. The review also highlighted the increasing need for trustworthy AI principles, including explainability, fairness, governance, privacy preservation, and humanistic security awareness, to guarantee the reliability of AI deployment. The study ultimately found that hybrid generative defense architectures that combine diffusion models, federated learning, explainable AI, graph neural networks, and adaptive semantic verification mechanisms will gain in importance for future secure and trustworthy computer vision systems in next-generation intelligent environments, given the constantly evolving nature of adversarial attacks.

REFERENCES

[1] C. Yu, C. Yao, M. Pei, and Y. Jia, “Diffusion-based kernel matrix model for face liveness detection,” *Image Vis. Comput.*, vol. 89, pp. 88–94, 2019.

[2] S. R. Bista, “The Influence of Generative AI on Adaptive Malware Defense Systems,” 2019.

[3] A. A. Abbasi, M. Mazinani, and R. Hosseini, “Evolutionary-based image encryption using biomolecules operators and non-coupled map lattice,” *Optik*, vol. 219, p. 164949, 2020.

[4] A. A. Abbasi, M. Mazinani, and R. Hosseini, “Evolutionary-based image encryption using biomolecules operators and non-coupled map lattice,” *Optik*, vol. 219, p. 164949, 2020.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

[5] M. W. Mayorga *et al.*, "Enhancing public resistance to 'fake news' a review of the problem and strategic solutions," *Handb. Appl. Commun. Res.*, pp. 197–212, 2020.

[6] C. Tang *et al.*, "CGD: Multi-view clustering via cross-view graph diffusion," in *Proceedings of the AAAI conference on artificial intelligence*, 2020, pp. 5924–5931.

[7] K. S. DHORAJIYA, N. D. SANGHANI, and A. HAIDER, "Exploiting Generative AI-A Systematic Literature Review for the Methods and Strategies to Generate Restrictive AI Images," 2018.

[8] Y. Yi, Z. Zhang, L. T. Yang, C. Gan, X. Deng, and L. Yi, "Reemergence modeling of intelligent information diffusion in heterogeneous social networks: The dynamics perspective," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 828–840, 2020.

[9] P. S. S. Tissera and S. Choe, "Bio-inspired quorum sensing-based nanonetwork synchronization using birth-death growth model," *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6263–6275, 2020.

[10] S. S. Assaf, "Synthetic biology guidelines for diffusion based molecular communication," PhD Thesis, Universitat Politècnica de Catalunya, 2019.

[11] Z. Guo *et al.*, "Beyond vulnerabilities: A survey of adversarial attacks as both threats and defenses in computer vision systems," *ArXiv Prepr. ArXiv250801845*, 2025.

[12] H. Du *et al.*, "Spear or Shield: The Role of Generative AI in Intelligent Network Services," *IEEE Netw.*, 2025.

[13] Y. Huang *et al.*, "On the trustworthiness of generative foundation models: Guideline, assessment, and perspective," *ArXiv Prepr. ArXiv250214296*, 2025.

[14] C. Hu *et al.*, "Generative AI-Empowered Secure Communications in Space–Air–Ground Integrated Networks: A Survey and Tutorial," *IEEE Commun. Surv. Tutor.*, vol. 28, pp. 4156–4194, 2025.

[15] H. Du *et al.*, "Spear or shield: Leveraging generative AI to tackle security threats of intelligent network services," *ArXiv Prepr. ArXiv230602384*, 2023.

[16] M. Andreoni, W. T. Lunardi, G. Lawton, and S. Thakkar, "Enhancing autonomous system security and resilience with generative AI: A comprehensive survey," *IEEE Access*, vol. 12, pp. 109470–109493, 2024.

[17] A. Mitra, S. P. Mohanty, and E. Kougianos, "Deepfakes and Large Language Models: Risks, Defenses, and the Future of Generative AI," *Authorea Prepr.*, 2026.

[18] Y. Jiang *et al.*, "Never compromise to vulnerabilities: A comprehensive survey on ai governance," *ArXiv Prepr. ArXiv250808789*, 2025.

[19] Q. Zhou and J.-B. Sheu, "The use of Generative Artificial Intelligence (GenAI) in operations research: Review and future research agenda," *J. Oper. Res. Soc.*, pp. 1–21, 2025.

[20] L. Zhang *et al.*, "Secure Semantic Communications via AI Defenses: Fundamentals, Solutions, and Future Directions," *ArXiv Prepr. ArXiv260222134*, 2026.

[21] Q. Li, X. Luo, Y. Chen, and J. Bjerva, "Trustworthy machine learning via memorization and the granular long-tail: A survey on interactions, tradeoffs, and beyond," *ArXiv Prepr. ArXiv250307501*, 2025.

[22] A. N. Kalejaiye, "Adversarial machine learning for robust cybersecurity: strengthening deep neural architectures against evasion, poisoning, and model-inference attacks," *Int. J. Comput. Appl. Technol. Res.*, vol. 13, no. 12, pp. 72–95, 2024.

[23] Z. Lu, W. Xu, C. Hua, M. Tu, and X. Xie, "Identity-Preserving Covert Communication With Generative Perturbation," *IEEE Trans. Netw. Sci. Eng.*, 2025.

[24] E. P. Fokkinga *et al.*, "Class-specific diffusion models improve military object detection in a low-data domain," *ArXiv Prepr. ArXiv260418076*, 2026.

[25] F. Zhu *et al.*, "Wireless large AI model: Shaping the AI-native future of 6G and beyond," *ArXiv Prepr. ArXiv250414653*, 2025.

[26] R. Almarwani, M. Almarwani, and F. Almarwani, "AI-Driven Synthetic Threats in Cybersecurity: A User-Centered Framework for Awareness, Detection, and Protective Behavior," *IEEE Access*, 2026.

[27] S. Huai, Z. Xie, and J. Luo, "R 2 DShield: Robust Object Detection in Real-time via Bayesian Input Shielding," 2026.

[28] J. Fan, S. Tan, H. Gu, Z. Wang, and J. Lü, "Dynamic Hypernetwork Grouping with Diffusion-Based Sampler for Heterogeneous Federated Intrusion Detection," *IEEE Internet Things J.*, 2026.

[29] C. Wu-Mo, A. Flores-González, J. Meléndez-Delgado, V. Ortiz-Gómez, H. Meléndez-González, and R. Maldonado-Hernández, "Artificial Intelligence-Driven Discovery and Optimization of Antimicrobial Peptides Targeting ESKAPE Pathogens and Multidrug-Resistant Fungi," *Microorganisms*, vol. 14, no. 3, p. 591, 2026.

[30] J. Poliner, "Generative Modeling With Sparse Data for Solid Mechanics," PhD Thesis, Columbia University, 2025.

[31] L. Zheng *et al.*, "Contingency Planning for Safety-Critical Autonomous Vehicles: A Review and Perspectives," *ArXiv Prepr. ArXiv260114880*, 2026.

[32] G. A. Noghre, "Real-World Privacy Preserving Human-Centric Video Anomaly Detection for Public Safety," PhD Thesis, The University of North Carolina at Charlotte, 2025.

[33] K. E. Wu, *Deep Learning: A Computational Modeling Toolbox for Biological Insight, Discovery, and Generation*. Stanford University, 2024.

[34] Y. Hao, "Are All Prior Art References Becoming Analogous in the AI Age?," *Available SSRN 6098327*, 2026.

[35] H. Zhang, S. Shen, Q. Cao, X. Wu, and S. Liu, "Modeling and analyzing malware diffusion in wireless sensor networks based on cellular automaton," *Int. J. Distrib. Sens. Netw.*, vol. 16, no. 11, p. 1550147720972944, 2020.