

Emerging Trends in Deep Learning-Based Image Encryption: A Survey

Nandish M¹, Mohan H G¹, Jalesh Kumar¹

¹Dept. of CSE., JNNCE Shivamogga, Visvesvaraya Technological University, Belagavi – 590018

Abstract - With the exponential growth of digital communication and data exchange, image security has emerged as a critical concern across domains such as healthcare, military, social media, and surveillance. With this surge, ensuring the authenticity and security of these images has become a critical concern for researchers. Traditional encryption methods, while widely used, face limitations when applied to the growing volume and complexity of image data. As a result, the use of deep learning (DL) models for image encryption has gained significant attention due to their adaptability and advanced capabilities. This paper offers a detailed review of recent developments in image encryption that leverage DL approaches. First, we present our motivations on the use of deep learning to secure images and the mutual advantages that arise for both the researchers in this field and the final users. Afterward, we investigate several state-of-the-art DL-based encryption approaches, with a summary of their major procedures and the salient characteristics that distinguish each one. In this regard, we present a comparison that unifies the most representative contributions in the state-of-the-art. Then, in comparison with other surveys in the field, we discuss the most representative open challenges and potential future research directions, including the urgency of setting a unified standard of evaluation for the security of DL-based image encryption.

Key Words: Image security, machine learning, deep learning, Encryption

1.INTRODUCTION

The ongoing development of Internet-based technologies contributed to an increase in the use of digital images as a medium of multimedia in most areas, such as communication, education, and entertainment, among others [1]. Digital images are preferred by people due to the possibility of understanding and transmitting messages quickly and intuitively, without having to read a large amount of text or additional information, or to extract the message from visual noise and semantic ambiguity [2]. The human brain is optimally designed for the recognition and memorization of images. In addition, learning in a visual context is now the most powerful way of teaching people how to best remember things. Currently, it is not uncommon for researchers to employ generative artificial intelligence solutions, for instance, ChatGPT model, to generate an image from text in applications to education, scientific research, and media industry. A 2023 report on AI-generated image statistics [3] revealed that users generate over 34 million images daily using OpenAI's DALL-E system.

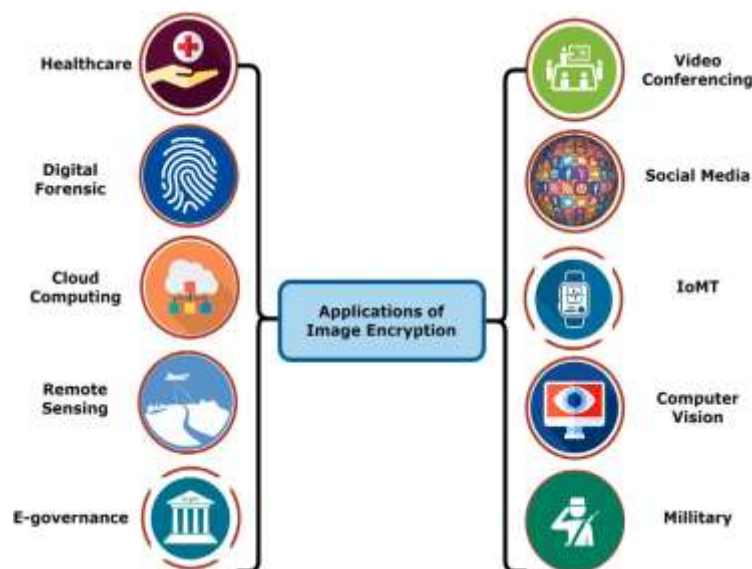


Fig- 1 Image encryption applications

The widespread use of social media—now involving over 5 billion users worldwide—has significantly contributed to the surge in digital image sharing, reflecting its central role in online communication [4]. However, as the use of digital images continues to grow, so do the risks associated with their misuse. Images shared or stored without proper security are vulnerable to various types of attacks, leading to privacy breaches [5]. This issue is especially critical in sensitive fields such as medical imaging, digital evidence handling, and biometric systems like facial recognition [6–8]. To address these concerns, image encryption plays a vital role in safeguarding image privacy [9]. This process converts readable images into seemingly random, unreadable data—often appearing as noise—so unauthorized users cannot interpret the original content. As illustrated in Fig. 1, image encryption is applied in numerous critical areas including healthcare, law enforcement, satellite imaging, e-governance, military systems, and social media platforms. Over time,

researchers have developed a variety of encryption techniques, each with its own strengths and weaknesses. Broadly, encryption methods fall into two categories: symmetric and asymmetric encryption. When the encryption and decryption keys are the same, it is referred to as symmetric encryption. If the keys are different, it is classified as asymmetric encryption.

2. LITERATURE REVIEW

The rapid evolution of deep learning has driven notable breakthroughs in image encryption, positioning Convolutional Neural Networks (CNNs) and Graph Neural Networks (GNNs) as key architectures in this domain. These models are particularly effective due to their capacity to learn intricate spatial hierarchies and nonlinear transformations, enabling robust encryption mechanisms that outperform traditional schemes. CNNs, in particular, have been widely adopted for generating secure image transformations owing to their feature extraction capabilities and adaptability to various image formats. Raghuvanshi et al. [10] introduced a CNN-based encryption scheme that integrates DNA encoding with logistic chaotic maps for cryptographic key generation. The approach exhibits high robustness against statistical and differential cryptanalytic attacks, making it suitable for security-critical applications. In another study, Bigdeli et al. [11] presented an innovative image encryption framework based on Convolutional Neural Networks (CNNs), specifically designed to support covert communication scenarios. Their model introduced a novel element by incorporating a chaotic tent map as an activation function within the CNN architecture, aiming to increase the system's unpredictability and nonlinearity. This integration of chaos theory into the deep learning process was intended to generate highly sensitive and dynamic transformations, thereby enhancing the obfuscation of visual data.

Chen et al. [12] developed a novel encryption model utilizing a fractional-order discrete chaotic neural network (FODCNN), which was augmented with DNA operations to enhance both scrambling and diffusion capabilities. This hybrid approach successfully improved the uniformity and sensitivity of the encrypted output. A fuzzy cellular neural network (FCNN) integrated with a chaotic system was used in [13] to construct robust encryption keys resistant to brute-force attacks. The model demonstrated a substantial key space, offering formidable resistance to brute-force attacks and showcasing its potential for large-scale security deployments. In subsequent work, Chen et al. [14] combined CNN architecture with a two-dimensional sin-linear-cosine (SLC) hyper-chaotic map. This configuration facilitated simultaneous compression and encryption of grayscale and color images. Their method successfully passed established randomness and security benchmarks, validating its effectiveness. Further expanding on this theme, Chen et al. [15] incorporated fractional Fourier transforms (FRFT) into a CNN-based framework, resulting in encrypted images with strong resilience to occlusion and blur distortions. This highlights the system's robustness in adverse conditions.

Bai et al. [16] proposed an image encryption model leveraging a CNN residual network in conjunction with Lorenz chaotic maps. Their approach significantly enhanced image reconstruction quality while preserving visual fidelity, even in encrypted form. In a privacy-critical domain, Mujeeb et al. [17] introduced a secure CNN-based framework for medical diagnostics. Their model employed discrete wavelet transforms (DWT) alongside cubic logistic chaotic maps, ensuring data privacy while maintaining diagnostic accuracy. A double-image encryption technique was developed in [18] by Man et al., utilizing the synergy of a five-dimensional chaotic system and CNN architecture for improved resistance against plaintext attacks. This dual-layered encryption exhibited strong immunity to known plaintext attacks. Likewise, Li et al. [19] presented a CNN-based model for encrypting iris images, incorporating XOR operations and a key matrix for transformation. Despite promising initial results, the study lacked an in-depth robustness evaluation under diverse attack models.

Ni et al. [20] proposed a multi-image encryption system that fused compressed sensing (CS) with CNNs, enabling efficient image compression and reliable recovery. This approach offered a dual advantage of storage optimization and data confidentiality. In another contribution, Wang et al. [21] embedded DNA encoding principles within a CNN-based encryption mechanism for color images. The resulting system exhibited high resilience to brute-force and statistical attacks, reinforcing its viability for practical use. Erkan et al. [22] developed a comprehensive encryption framework that employed deep CNNs alongside a chaotic logarithmic map. Their model integrated permutation, diffusion, and DNA encoding rules, demonstrating robust encryption quality under varied evaluation metrics. In [23], a secure CNN-based encryption model was introduced by Abdellatif et al. for CT images, employing chaotic sequences and magic transformations to ensure the confidentiality and integrity of healthcare data.

In parallel, Generative Adversarial Networks (GANs) have become increasingly popular for image encryption, largely due to their capacity to model complex data distributions and generate high-entropy transformations. These networks offer dynamic key generation and content-aware encryption, enhancing overall system robustness. Singh et al. [24] pioneered a GAN-based encryption framework that integrates a customized super-resolution network (CSRNet) with chaotic map-driven key generation. The model's ability to produce real-time secure image transformations makes it ideal for latency-sensitive applications. Ding et al. [25] introduced DLEDNet, a GAN-based encryption framework tailored for the Internet of Medical Things (IoMT). By incorporating robust key generation mechanisms, the model enables secure data transmission and reconstruction even under adversarial conditions, including architecture-aware attacks.

Dev Singh et al. [26] proposed a highly randomized GAN-based encryption process that systematically applies substitution, permutation, and diffusion transformations. The model demonstrated strong resilience against various cryptographic attacks, including chosen-plaintext and differential analysis. Similarly, Fang et al. [27] enhanced the encryption process by integrating a hyper-chaotic system into the GAN architecture, resulting in elevated randomness and fortified data protection. Bao et al. [28] presented an

innovative encryption method that combines autoencoders with CycleGAN in an asymmetric cryptographic setup. Although their system effectively maintained image reconstruction quality, it did not thoroughly assess computational efficiency or deployment scalability. Man et al. [29] designed an encryption technique based on Least Squares GANs (LSGAN) and six chaotic systems to optimize pseudorandom key sequences. Their model successfully passed standard randomness evaluations, attesting to its encryption quality. Ding et al. [30] developed DeepKeyGen, a GAN-powered stream cipher designed for encrypting medical images. The system supports large key spaces and delivers fast encryption, making it highly suitable for secure telemedicine platforms. Panwar et al. [31] introduced Encipher GAN, wherein the encryption key is generated using GANs and decryption is guided by a customized loss function. Their model showed notable success in defending against plaintext and ciphertext attacks.

Fang et al. [32] proposed a hybrid model that combines a deep convolutional GAN with a hyper-chaotic system to secure multimedia content. The architecture was evaluated under various threat models and demonstrated significant resistance to brute-force and plaintext attacks. In a separate study, Sirichotedumrong and Kiya [33] employed GANs alongside ResNet-18, trained on the CIFAR-10 dataset, to generate robust ciphers. However, their study lacked a detailed security performance analysis. Neela and Kavitha [34] presented a secure image encryption model integrating blockchain with GANs for medical image transmission in cloud environments. The GAN was utilized for dynamic key generation, while blockchain ensured data authenticity and immutability. Mulkiah et al. [35] introduced a compression-then-encryption paradigm utilizing GANs in conjunction with logistic maps. Although this approach offered high-security levels, it incurred substantial computational overhead, which may hinder real-time applications. The system passed the NIST randomness tests, affirming its effectiveness in securing diagnostic imagery while preserving relevant clinical information.

Table 1: Summary of CNN and GAN-Based Image Encryption Techniques

Ref No.	Objectives	Techniques and Deep Learning Models	Role of Deep Learning	Datasets
[10]	Secure image encryption using biological and neural systems	CNN with DNA encoding and logistic maps	CNN helps in encoding pixel values and generating dynamic keys	--
[11]	Covert communication via neural encryption	CNN with chaotic tent map as activation	CNN simulates chaotic behavior for secure encryption	--
[12]	Enhance encryption robustness for color images	FODCNN + DNA operations	FODCNN improves image scrambling and diffusion strength	--
[13]	Improve resistance against brute-force attacks	FCNN within chaotic system	Neural networks generate secure key sequences	--
[14]	Visual image encryption using chaos and learning	CNN + 2D SLC hyper-chaotic map	CNN compresses and encrypts, enhancing robustness	--
[15]	Robustness against occlusion/blur in encrypted images	CNN + FRFT	CNN improves reconstruction post-decryption	--
[16]	Reconstruction of encrypted grayscale images	CNN Residual Network + Lorenz chaos	Residual CNN improves decryption quality	--
[17]	Privacy-preserving medical diagnosis	CNN + DWT + chaotic maps	CNN classifies and helps in secure diagnosis encryption	Medical data (not named)
[18]	Double-image encryption	CNN + 5D chaotic system	CNN aids in complex multi-image encryption layers	--
[19]	Iris image encryption	CNN + XOR + key derivation	CNN extracts features for secure transformation	Iris image dataset
[20]	Multi-image encryption with efficiency	CNN + Compressed Sensing + Gyrator domain	CNN facilitates recovery after encryption	--

[21]	Color image encryption with genetic principles	CNN + DNA sequence operations	CNN guides DNA-based encoding of RGB values	--
[22]	Secure CNN-based encryption framework	Deep CNN + chaotic log map	CNN models used for permutation and diffusion	--
[23]	Medical CT image encryption	CNN + chaotic maps + magic transforms	CNN ensures privacy of sensitive medical content	CT image dataset
[24]	Real-time image encryption using GAN	GAN + CSRNet + chaotic maps	GAN generates random keys; CSRNet refines output	--
[25]	IoMT encryption and decryption	GAN (DLEDNet) + reconstruction network	GAN learns secure mappings; reconstruction ensures clarity	IoMT data (unspecified)
[26]	Secure image encryption with high randomness	GAN + permutation + diffusion	GAN generates dynamic keys with high entropy	--
[27]	Enhance robustness via chaotic enhancement	GAN + hyper-chaotic system	GAN aids in generating chaotic sequences	--
[28]	Secure multimedia encryption	CycleGAN + autoencoder	GAN creates keys, while autoencoder scrambles images	--
[29]	Random number generation for encryption	LSGAN + chaotic systems	GAN tunes chaotic sequences for stronger keys	--
[30]	Medical stream cipher generator	GAN (DeepKeyGen)	GAN learns to create cipher streams for encryption	Medical image datasets
[31]	End-to-end color image encryption	Encipher GAN + SGD optimization	GAN generates secure keys and reconstructs decrypted images	--
[32]	Robust hybrid GAN-based encryption	DCGAN + hyper-chaotic system	GAN models generate pseudo-random sequences	--
[33]	Privacy-preserving deep learning encryption	ResNet-18 + GAN	GAN transforms images, ResNet measures classification	CIFAR-10
[34]	Cloud-secure encryption for medical images	GAN + blockchain	GAN for key generation; blockchain ensures authenticity	--
[35]	Compression + encryption framework	GAN + logistic map	GAN compresses; logistic map encrypts the image	--

3. CHALLENGES AND POSSIBLE SOLUTION

Despite the promising advancements in deep learning-based image encryption, several critical challenges remain unresolved in both practical deployment and theoretical robustness. One of the foremost challenges lies in the computational overhead introduced by complex CNN and GAN architectures. As observed in Mulkiah et al. [35], although their GAN-based model achieves high security, the encryption process demands substantial computational resources, limiting its applicability in low-power or real-time systems. A potential solution involves model compression techniques such as pruning or quantization, which can reduce the model size without significant compromise on security. Secondly, robustness against adaptive attacks is a key concern. While approaches like that of Dev Singh et al. [26] and Man et al. [29] incorporate chaotic systems to enhance randomness, attackers may still exploit known

vulnerabilities in neural network behaviors. Introducing adversarial training during the model development phase could increase resistance against such threats.

Key generation and management by neural networks is also not well-defined. GANs are the most used neural network for this purpose as is the case in [24], [25] and [30] but in most of them the issues of reproducibility and security of generated keys are not addressed. A viable direction is integrating blockchain frameworks like in Neela and Kavitha [34] to validate the key generation process and ensure non-repudiation. Many encryption schemes, such as those proposed in [19] and [33], lack a thorough security evaluation like randomness testing or differential analysis. This omission leaves their reliability questionable. A recommended solution is adopting standardized testing protocols such as NIST SP800-22 to benchmark the quality of encryption rigorously. Additionally, dataset dependence affects the generalization of encryption models. Several works including Sirichotedumrong and Kiya [33] rely on small or fixed datasets (e.g., CIFAR-10), which may not cover broader visual patterns. This issue could be alleviated by training and validating models on diverse and large-scale datasets, including medical and multimedia images. Moreover, many models, such as those in [11] and [28], either lack performance benchmarks or fail to compare against classical encryption methods. To ensure credibility, it's necessary to establish unified benchmarks that allow for fair comparison in terms of encryption speed, quality, and robustness.

Another key limitation lies in the visual quality of decrypted images, especially for sensitive domains like medical imaging. Although CSRNet was applied by Singh et al. [24] to enhance decrypted outputs, a more widespread adoption of super-resolution and perceptual enhancement networks could significantly improve practical usability. Chaotic systems are widely employed across surveyed models for improving entropy, yet parameter sensitivity remains a bottleneck. Even slight deviations may lead to failure in decryption. Hybridizing deterministic chaos with learnable models, or introducing error-tolerant decoding techniques, could mitigate this challenge. While GANs are powerful, their training instability is well-known and affects the encryption model's reliability. Techniques such as Wasserstein loss functions or least-squares GANs (as used in [29]) provide more stable training and should be considered standard practice. There's also limited exploration of real-time applicability, with most models focusing solely on theoretical strength. Models like those of Singh et al. [24] are suitable for real-time environments, indicating that integrating lightweight architectures with hardware acceleration (like edge TPU or FPGA) can address this need. Interpretability of the encryption mechanism is another pressing concern. Deep models often act as black boxes, making it hard to understand how security is being achieved. Employing explainable AI (XAI) techniques could help demystify these models and support their trustworthiness.

Cross-domain applicability, such as encrypting images across different modalities (medical, satellite, surveillance), remains underexplored. Research should move towards domain-adaptive encryption frameworks using transfer learning. Most importantly, legal and ethical concerns are rarely addressed. Encryption frameworks involving personal data, especially in healthcare [25], [30], must ensure compliance with standards like HIPAA and GDPR, and future models should incorporate privacy-by-design principles. Lastly, very few works address multi-user or hierarchical access encryption, which is vital in collaborative environments. Future schemes could incorporate multi-level GANs that generate user-specific keys with layered access permissions. In conclusion, while CNN and GAN-based image encryption systems offer impressive capabilities, addressing these challenges through a mix of algorithmic innovation, standardized evaluation, and ethical design is critical to their broader adoption and trust in real-world applications.

4. CONCLUSION

This survey provides a comprehensive overview of recent advancements in deep learning-based image encryption, highlighting the growing importance of secure visual data transmission in domains such as healthcare, military, and digital communications. By reviewing both CNN and GAN-driven approaches, we observed how deep learning models enhance encryption strength through adaptive feature learning, chaos integration, and robust key generation. However, despite notable achievements, several challenges persist—ranging from high computational costs and limited generalizability to the lack of standardized evaluation metrics and interpretability. Addressing these issues requires interdisciplinary research that combines cryptography, deep learning, and hardware optimization. Future work should also prioritize real-time deployment, legal compliance, and cross-domain applicability. Overall, this study underscores the potential of deep learning as a transformative tool for next-generation image security while encouraging more rigorous, efficient, and transparent solutions.

REFERENCES

- [1]. M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 3, pp. 1617–1655, 2016.
- [2]. A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surv. Tutor.*, vol. 18, no. 2, pp. 1153–1176, 2015.
- [3]. "AI image statistics: How much content was created by AI," *Everyapixel Journal*, 2023. [Online]. Available: <https://journal.everyapixel.com/ai-image-statistics>. [Accessed: Dec. 18, 2023].

- [4]. S. Kemp, "Digital 2023: Global overview report," *DataReportal – Global Digital Insights*, 2023. [Online]. Available: <https://datareportal.com>. [Accessed: Dec. 18, 2023].
- [5]. O. P. Singh, A. K. Singh, G. Srivastava, and N. Kumar, "Image watermarking using soft computing techniques: A comprehensive survey," *Multimedia Tools Appl.*, vol. 80, pp. 30367–30398, 2021.
- [6]. A. Anand and A. K. Singh, "Watermarking techniques for medical data authentication: A survey," *Multimedia Tools Appl.*, vol. 80, pp. 30165–30197, 2021.
- [7]. M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, 2016.
- [8]. X. Chen et al., "Covert communications: A comprehensive survey," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 2, pp. 1173–1198, 2023.
- [9]. O. Singh and A. K. Singh, "Data hiding in encryption," *Multimedia Tools Appl.*, forthcoming.
- [10]. K. K. Raghuvanshi, S. Kumar, S. Kumar, and S. Kumar, "Image encryption algorithm based on DNA encoding and CNN," *Expert Syst. Appl.*, vol. 252, p. 124287, 2024.
- [11]. N. Bigdeli, Y. Farid, and K. Afshar, "A novel image encryption/decryption scheme based on chaotic neural networks," *Eng. Appl. Artif. Intell.*, vol. 25, no. 4, pp. 753–765, 2012.
- [12]. L.-P. Chen et al., "A novel color image encryption algorithm based on a fractional-order discrete chaotic neural network and DNA sequence operations," *Front. Inf. Technol. Electron. Eng.*, vol. 21, no. 6, pp. 866–879, 2020.
- [13]. K. Ratnavelu et al., "Image encryption method based on chaotic fuzzy cellular neural networks," *Signal Process.*, vol. 140, pp. 87–96, 2017.
- [14]. W. Chen et al., "Explore the potential of deep learning and hyperchaotic map in the meaningful visual image encryption scheme," *IET Image Process.*, vol. 17, no. 11, pp. 3235–3257, 2023.
- [15]. J. Chen, X.-W. Li, and Q.-H. Wang, "Deep learning for improving the robustness of image encryption," *IEEE Access*, vol. 7, pp. 181083–181091, 2019.
- [16]. X. Bai et al., "Reconstruction of chaotic grayscale image encryption based on deep learning," in *Proc. IEEE Int. Conf. Imaging Syst. Techn.*, 2021, pp. 1–6.
- [17]. Mujeeb et al., "A novel chaos-based privacy-preserving deep learning model for cancer diagnosis," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 6, pp. 4322–4337, 2022.
- [18]. Z. Man et al., "Double image encryption algorithm based on neural network and chaos," *Chaos Solitons Fractals*, vol. 152, p. 111318, 2021.
- [19]. X. Li et al., "Research on iris image encryption based on deep learning," *EURASIP J. Image Video Process.*, vol. 2018, no. 1, pp. 1–10, 2018.
- [20]. R. Ni et al., "Multi-image encryption based on compressed sensing and deep learning in optical gyrator domain," *IEEE Photonics J.*, vol. 13, no. 3, pp. 1–16, 2021.
- [21]. J. Wang, F. Long, and W. Ou, "CNN-based color image encryption algorithm using DNA sequence operations," in *Proc. Int. Conf. Security, Pattern Anal., Cybernetics (SPAC)*, IEEE, 2017, pp. 730–736.
- [22]. U. Erkan et al., "An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN," *Multimedia Tools Appl.*, vol. 81, no. 5, pp. 7365–7391, 2022.
- [23]. E. Abdellatef, E. A. Naeem, and F. E. A. El-Samie, "DeepEnc: deep learning-based CT image encryption approach," *Multimedia Tools Appl.*, 2023.
- [24]. M. Singh, N. Baranwal, K. N. Singh, and A. K. Singh, "Using GAN-based encryption to secure digital images with reconstruction through customized super resolution network," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3977–3984, 2024.
- [25]. Y. Ding et al., "DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1504–1518, 2020.
- [26]. O. D. Singh et al., "A robust and secure immensely random GAN based image encryption mechanism," *Multimedia Tools Appl.*, vol. 82, no. 13, pp. 19693–19743, 2023.
- [27]. P. Fang, H. Liu, C. Wu, and M. Liu, "A block image encryption algorithm based on a hyperchaotic system and generative adversarial networks," *Multimedia Tools Appl.*, vol. 81, no. 15, pp. 21811–21857, 2022.
- [28]. Z. Bao, R. Xue, and Y. Jin, "Image scrambling adversarial autoencoder based on the asymmetric encryption," *Multimedia Tools Appl.*, vol. 80, no. 18, pp. 28265–28301, 2021.
- [29]. Z. Man et al., "A novel image encryption algorithm based on least squares generative adversarial network random number generator," *Multimedia Tools Appl.*, vol. 80, pp. 27445–27469, 2021.
- [30]. Y. Ding et al., "DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 9, pp. 4915–4929, 2021.
- [31]. K. Panwar et al., "Encipher GAN: An end-to-end color image encryption system using a deep generative model," *Systems*, vol. 11, no. 1, p. 36, 2023.

- [32]. P. Fang, H. Liu, and C. Wu, "A novel chaotic block image encryption algorithm based on deep convolutional generative adversarial networks," *IEEE Access*, vol. 9, pp. 18497–18517, 2020.
- [33]. W. Sirichotedumrong and H. Kiya, "A GAN-based image transformation scheme for privacy-preserving deep neural networks," in *Proc. Eur. Signal Process. Conf. (EUSIPCO)*, IEEE, 2021, pp. 745–749.
- [34]. K. Neela and V. Kavitha, "Blockchain based chaotic deep GAN encryption scheme for securing medical images in a cloud environment," *Appl. Intell.*, vol. 53, no. 4, pp. 4733–4747, 2023.
- [35]. A. K. Sari et al., "Compression-encryption model for digital images based on GAN and logistic map," in *Proc. Int. Seminar on Intelligent Technology and Its Applications (ISITIA)*, IEEE, 2021, pp. 319–324.