ENGINEERING SCIENCE

The International Journal of Engineering Sciences
Vol. 2, No. 1, 2025, pp. 1-8
ISSN 3104-8897

https://international-journal-of-engineering-sciences.jo

Innovative Image Encryption System Employing WGAN-GP with AES for Securing Transmission of Medical Images in IoT Environment

RANA SAEED HAMDI[(1)], SAIF AL-ALAK,[(2)] ELAF ALI ABOOD[(3)]
[1] College of Medicine-University of Babylon, Email: scw564.rana.saeed@student.uobabylon.edu.iq
[2] Department of Computer Science-College of Science for Women – University of Babylon, Email: saifmahmood@uobabylon.edu.iq
[3] Department of Computer Science-College of Science for Women – University of Babylon, Email: wsci.elaf.ali@uobabylon.edu.iq

* Corresponding Author: **RANA SAEED HAMDI**

DOI: https://doi.org/10.64440/INTERNATIONALENGINEERING-3104-8897/ENG001

ARTICLE INFO

Article history
Received June 02, 2025
Revised June 04, 2025
Accepted July 21, 2025

Keywords
cryptography;
WGAN-GP;
IOT;
medical images,
AES.

ABSTRACT

Images are essential digital assets in the application of IOT, such as medicine, transportation, farming, the armed forces, and smart city planning. However, ensuring secure transmission of images over IoT networks remains a challenge due to key generation vulnerabilities and reliance on mathematically complex cryptographic systems. This paper proposes a new encryption scheme combining Wasserstein Generative Adversarial Networks with Gradient Penalty (WGAN-GP) for random key generation, used with the AES encryption algorithm.

The randomness of the generated keys was verified using NIST and Diehard tests, demonstrating good statistical quality. Experimental results confirm the efficacy of the scheme: the encrypted images showed entropy values approaching 8.0 indicating a very high degree of randomness; PSNR values were around 6.12 dB and MSE values were above 105 indicating very strong encryption data distortion; histogram analyses showed the outputs had uniform distributions; and correlation coefficients were shown to be close to zero, thereby demonstrating the scheme was resistant to statistical attacks and spatial attacks. Decryption led to lossless reconstruction characterized by infinite PSNR and MSE of zero.

Overall, the results presented in this study demonstrate the scheme's robustness, efficiency in the encryption and decryption process, and applicability for protecting sensitive image data in IoT networks..

ENGINEERING SCIENCE
The International Journal of Engineering Sciences
https://international-journal-of-engineering-sciences.jo
Vol. 2, No. 1, 2025, pp. 1-8
ISSN 3104-8897

1. Introduction

The Internet of Things includes a wide variety of devices and diverse link layer technologies [1]. IOT applications are growing in number in recent times [2]. Smart homes, cities, agriculture, utilities, healthcare monitoring, animal husbandry, water, industrial control, management, security and emergencies, transportation, and environment monitoring are among the applications [3]. It addresses extremely secret information regarding individuals and corporations, which must remain undisclosed to unauthorized individuals or adversaries.

IoT technology security is a challenging task, and security is a crucial issue that may have an effect on the IoT's future development. Additionally, Confidentiality, availability, authenticity, authorization, and access control are security requirements in an IoT environment [4,5].

A process called cryptography turns readable data into unintelligible (encrypted) data that only the owner of the decryption key can decode. Since the data is frequently confidential or extremely important, the main goal of encryption is to protect data privacy by preventing unwanted access or alteration [6].

Symmetric (the key for encryption and decryption is identical) and asymmetric (the keys for encryption and decryption are distinct) are fundamental categories in cryptography, whereas lightweight is a contemporary category aimed for lower-end devices. Numerous cryptographic algorithms and security approaches serve as the foundation for a number of the lightweight security solutions in use. They consist of lightweight public-key cryptography systems built on ECC (Elliptic Curve Cryptography), The hash functions like access control, and The xor encryption [7], and symmetric AES 128 algorithm, A worldwide Network for Microwave Access (WiMAX), and the Bluetooth [8,9].

To improve IoT security, machine learning techniques are becoming more popular as they make encryption and key generation procedures simpler, requiring less time and complexity[10,11,12]. The field of machine learning features Wasserstein Generative Adversarial Networks with Gradient Penalty (WGAN-GP) as deep generative models. The system performs cryptographic key generation to enhance image communication security by generating stronger and more random keys.

The work combines strong randomness with multiple AES keys to improve image security through the Internet of Things. Measures like correlation, MSE, PSNR, and entropy show that the suggested WGAN-GP-AES can achieve higher levels of security and integrity.

The Related Work

To improve image security, several earlier investigations used symmetric single-key AES. Alireza et al. proposed a chaotic system for key generation and AES modifications [13]. In addition, Ahmed et.al. proposed combining an AES system with a shifting mechanism [14], and Jha proposed an image encryption method that corresponds to AES and utilizes a 2-D logistic map [15]. All of these attempts to improve upon the inherent flaws in single-key standard AES aim to achieve one of two things: either increase the key's randomness or make some modifications to the original AES.

In [14] 2019, Haidar proposed a secure approach for encrypting images that uses AES in combination with the Haar wavelet transform and pixel shuffling grounded in a chaotic logistic map.

In contrast, Khizrai and Mohsen employed multiple key schemes [16,17] to enhance the security level. Mohammed and Al-alak (2018) suggested a hybrid system utilizing an asymmetric algorithm to generate a secret key for the encryption of data transferred in a Wireless Sensor Network (WSN) [18]. In 2021, Hussein and Al-alak proposed reducing the complexity of the random number generator by employing lightweight techniques to generate secret keys [19]. In 2021, Salim et al. introduced an MECCAES algorithm that enhances IoT image security by addressing issues associated with single-key image encryption. The experimental tests demonstrate that the new system demonstrates confidential performance [1]. Ji and colleagues from 2022 designed a system through chaotic systems and Generative Adversarial Networks to generate pseudo-random sequences. The GAN model demonstrates high levels of unpredictability and chaos when it undergoes multiple training iterations on specific randomization parameters, which enables its use in encryption systems [20].

Park et al in 2022 sought to improve random number generator performance. The researchers achieved their goal through the creation of a hybrid PRNG model. They implemented convolutional neural networks together with reinforcement learning algorithms. The model demonstrated its capability to produce highly random sequences by achieving a maximum correlation coefficient of 19% [21]. In 2020, a network called DeepKeyGen, which uses deep learning for medical image encryption, was established as a high-security level prototype. The results of three different datasets showed that Deep Learning could become integrated with cryptographic operations by generating private keys [22].

In 2012, Desai et al. prepared random sequences through a layer recurrent neural network (LRNN) that utilized weight matrices. The researchers found that the sequences successfully passed 11 out of 16 NIST statistical tests while their performance differed according to the selected training function [23]. This study improves the security of transferred images by using AES key combination with several keys that are highly random. This research primarily focuses on enhancing image security in IoT applications with AES encryption. Wasserstein Generative Adversarial Networks with Gradient Penalty (WGAN-GP) ensures elevated security and integrity, as shown by statistical metrics like Entropy, PSNR, MSE, and correlation.

2. Theoretical Background

1. Cryptography

Cryptography is a crucial way for ensuring data security, particularly for protecting end-to-end data transmitted over networks [18,24]. The process of encrypting text or other data so that it can only be read by a person in possession of the decryption key is known as cryptography. Encryption prevents unauthorized parties from accessing or tampering with sensitive data due to its significance.

As will be explained below, symmetric and asymmetric types are critical in the field of cryptography:

- **Asymmetric Key Algorithm**

ENGINEERING SCIENCE
The International Journal of Engineering Sciences
https://international-journal-of-engineering-sciences.jo
Vol. 2, No. 1, 2025, pp. 1-8
ISSN 3104-8897

This is sometimes known as the Public Key Algorithm. Two distinct keys exist: one public and one private, which are mathematically interconnected. The public key facilitates the encryption of the message by the transmitter, while the private key is employed by the receiver for decryption purposes. Upon sending the message, the sender encrypts it using the public key and transmits this key to the receiver. The only entity capable of decrypting the message is the recipient's private key, which must remain confidential and never be disclosed.

- **Symmetric Key Algorithm**

This method is known as secret key cryptography because the same secret key is used for encryption and decryption [25,26]. Symmetric key cryptosystems can be further categorized into two primary kinds: block ciphers and stream ciphers. In stream ciphers, each bit is combined with the relevant key bit stream; while in a block ciphers many message bits are combined together and then combined with all of the key bits [27]. Asymmetric algorithms are more complex to implement and require more resources than symmetric algorithms [28].

Advanced Encryption Standard (AES) is widely employed the symmetric key encryption algorithm, designed to ensure data confidentiality and recognized for its high level of security [19].

The most significant security concern in symmetric encryption systems is the utilization of a single static key. If this key becomes compromised, the entire encrypted conversation is threatened. Conventional symmetric systems, albeit efficient, are plagued by predictability and key reuse vulnerabilities, particularly in IoT contexts where secure key management is challenging [29].

The proposed method addresses its limitation through the implementation of machine learning techniques that produce various encryption keys. Multiple keys boost security measures by lowering the chances of failure at a single point while simultaneously increasing randomness.

1. AES Algorithm

The Advanced Encryption Standard (AES) is a widely utilized the symmetric block cipher method in cryptography. Encrypting data with the AES algorithm renders it exceedingly challenging for hackers to retrieve the original information. The AES method permits three key sizes: 128, 192, and 256 bits; however, the block size for messages is set at 128 bits [30,31].

3.Random Key Generation

3.1 The Wasserstein Generative Adversarial Networks with Gradient Penalty (WGAN-GP):

Gradient Penalty in the Wasserstein Generative Adversarial Network (WGAN-GP) In machine learning, they belong to a class of deep generative models. In order to improve randomness (by lowering redundancy), reduce complexity, and subsequently decrease the security of the transmitted image, it is used for generating stronger and more effective cryptographic keys.

In complex distributed data, the generative adversarial network (GAN) shows promise for image denoising and feature extraction; yet, it has difficulties in training and has slow convergence. The training stability is improved using the Wasserstein GAN (WGAN) [32,33]. Algorithm 1 displays the WGAN-GP Model that was suggested. Figure 1 shows the proposed WGAN-GP Model.

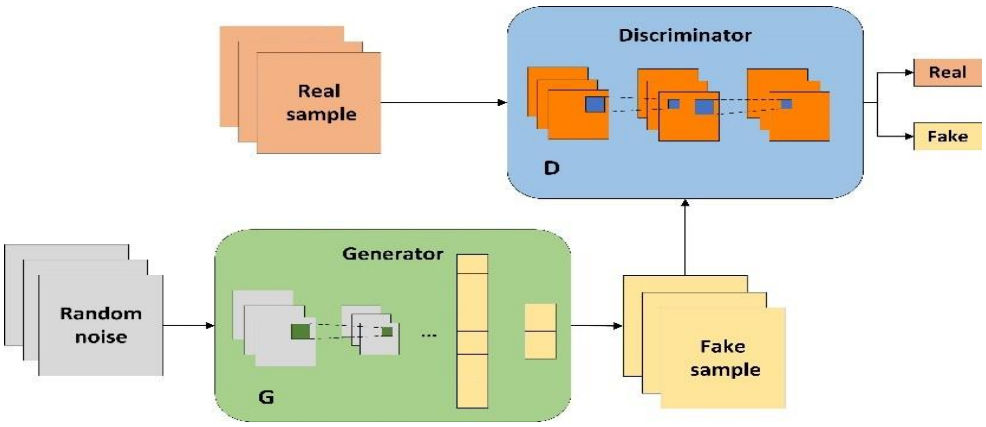

Figure 1: The WGAN-GP model architecture [34].

Theoretical Examination of the Effects of Technology on Efficiency

In order to illustrate how deploying efficiency-improving technologies affects network performance, this analysis depends on theoretical models that interact. In order to determine the best operating levels and forecast possible outcomes using theoretical models, this analysis makes use of positive equations and theories. With idealized assumptions that assist eliminate ambiguity and offer a clear theoretical picture of how to increase efficiency using just theoretical tools and concepts, the models incorporate theoretical variables and parameters [16].

3. Theoretical Structure for Assessing Efficiency and Performance

Evaluation of performance and efficiency is a key concern that necessitates the creation of comprehensive theoretical models in order to comprehend and assess the efficacy of the mechanisms and technologies employed in smart grids. Here, the theoretical framework is based on developing a set of standards and hypotheses that allow for the assessment of electrical performance, the calculation of efficiency levels, and the systematic and deductive analysis of the effects of contemporary technologies without the need for field data or actual experiments.

3.1. Standards for Electrical Performance

The theoretical framework starts by outlining a set of standards and metrics for gauging smart grid effectiveness and performance. These standards are developed using theoretical and mathematical models, such as [17]:

- Energy efficiency, which can be mathematically stated using the following formula, is defined as the ratio of power input to power used from the grid: [\frac{\text{Useful Power}} = \eta] {\text{Power Input}}/]

- Electrical circuit theory-based equations are used to express energy loss, which is programmed as a function of resistance, currents, and operating circumstances.

The International Journal of Engineering Sciences
https://international-journal-of-engineering-sciences.jo
Vol. 2, No. 1, 2025, pp. 1-8
ISSN 3104-8897

- Power balance equations and fluctuation projections are used to evaluate load quality, which is the stability and balance of electrical currents and voltages.

- Reliability, it is theoretically modeled using probabilistic models and contingency theories based on the likelihood of failure and unplanned outages.

3.2. Theories and Models for Evaluating Efficiency

Several ideas serve as the foundation for efficiency evaluation models, including [18]:

- Network theory is the study of power distribution, voltages, and currents using linear and nonlinear network equations that characterize the network's theoretical state.

- Control theory and dynamic models are used to assess system responsiveness and stability, examine network response, and accomplish dynamic load-to-production balance.

- Probability and statistics: To assess dependability, forecast technological malfunctions, and employ probabilistic hypotheses to examine system flaws.

- Models for the Evaluation of Theoretical Efficiency: to incorporate cognitive measurement equations that, under the assumption of the ideal or theoretical dynamic state, relate the performance of system components (such as fans, switches, and distribution systems) to the system's overall performance.

3.3. A Theoretical Examination of How Contemporary Technologies Affect Efficiency

The theoretical conclusions drawn from mathematical and theoretical models form the basis of this investigation. Ideally or theoretically, the effects of any contemporary technology are anticipated and assessed using temporal and geographical efficiency coefficients [19]:

- Using mathematical models from control theory and the assumption of an ideal steady state, the influence of smart load management is examined through theoretical hypotheses regarding distribution optimization and loss reduction.

- Using dynamic models that depict how sources interact with the grid and make assumptions about ongoing output variations and the optimal system response, the integration of renewable energy sources is assessed.

- Theoretical modeling of storage systems: depends on models of charging and discharging that are controlled by mathematical control theories and thermodynamics, presuming that the storage system is completely efficient.

3.4. Theoretical Assessment of Technology's Effect on Efficiency

This approach relies on deductive reasoning derived from theoretical deductions and mathematical models [20]:

- calculating the effects of every technology at the same time while accounting for theoretical presumptions about system performance.

- Create fictitious situations to examine the relationship between efficiency gains and technology deployment theoretically, keeping the conclusions limited to presumptions and theoretical constraints.

- Provide theoretical metrics for measuring continual improvement and examine how advancements in contemporary technology can raise performance levels in accordance with the theoretical frameworks described.

The theoretical framework, which is based on scientific ideas and mathematical models, offers a strong basis for comprehending and assessing smart grid performance. Establishing precise performance benchmarks and offering theoretical approximations of the effectiveness of contemporary systems and technologies are the goals of this approach. Based on models that can make rational, empirically backed predictions and conclusions, this aids in directing future development and improvement processes.

3.5. Benefits and Drawbacks of the Theoretical Structure

This framework's main benefit is its capacity to offer a thorough and methodical assessment grounded in theoretical and mathematical underpinnings, allowing for the comparison of various technologies using uniform standards. Its heavy reliance on theoretical presumptions and models, which might not adequately account for the intricacies of field reality and environmental changes, is one of its biggest drawbacks. Therefore, a supporting field research is always necessary when translating the results to real-world applications. To improve its realism and dependability, this framework can also be expanded to incorporate experimental data or computer models based on simulation.

As a result, the theoretical framework is a useful instrument for researching and evaluating smart grid efficiency. It also serves as a strong scientific basis that aids in the development of more dependable and efficient systems that meet future demands and are in line with continuing technological advancements [21].

4. Conclusion:

In this paper, researchers introduce a novel encryption scheme by integrating WGAN-GP-generated keys with the AES cipher to improve the security of image transmission in an IoT environment. The method utilizes WGAN-GP's powerful generative properties to produce highly random keys for encryption, thereby improving security and reducing predictability. The performance of the proposed approach has been validated through entropy analysis and PSNR/MSE evaluations. Additionally, histogram uniformity and correlation coefficient analysis were also employed. Results demonstrate that the proposed encryption scheme exhibits high randomness, strong quality, and resistance to attacks. Future work will focus on optimizing the efficiency of WGAN-GP for real-time applications and applying it to other cryptographic contexts.

Author Contribution: All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

[1] K. G. Salim, S. M. K. Al-alak, and M. J. Jawad, “Improved image security in internet of thing (IoT) using multiple key AES,” Baghdad Sci. J., vol. 18, no. 2, pp. 0417–0417, 2021.

The International Journal of Engineering Sciences
https://international-journal-of-engineering-sciences.jo
Vol. 2, No. 1, 2025, pp. 1-8
ISSN 3104-8897

[2] M. N. Halgamuge and D. Niyato, "Adaptive edge security framework for dynamic IoT security policies in diverse environments," Comput. Secur., vol. 148, p. 104128, Jan. 2025, doi: 10.1016/j.cose.2024.104128.

[3] Gunjan, S. Agarwal, D. Rai, and S. Talreja, "Applications of IoT in Smart Homes and Cities," in IoT Based Smart Applications, N. Sindhwani, R. Anand, M. Niranjanamurthy, D. Chander Verma, and E. B. Valentina, Eds., in EAI/Springer Innovations in Communication and Computing. , Cham: Springer International Publishing, 2023, pp. 55–70. doi: 10.1007/978-3-031-04524-0_4.

[4] V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A review of IoT security and privacy using decentralized blockchain techniques," Comput. Sci. Rev., vol. 50, p. 100585, Nov. 2023, doi: 10.1016/j.cosrev.2023.100585.

[5] G.-C. Lee, J.-H. Li, and Z.-Y. Li, "A Wasserstein Generative Adversarial Network–Gradient Penalty-Based Model with Imbalanced Data Enhancement for Network Intrusion Detection," Appl. Sci., vol. 13, no. 14, p. 8132, Jul. 2023, doi: 10.3390/app13148132.

[6] M. Kaur et al., "EGCrypto: A Low-Complexity Elliptic Galois Cryptography Model for Secure Data Transmission in IoT," IEEE Access, vol. 11, pp. 90739–90748, 2023, doi: 10.1109/ACCESS.2023.3305271.

[7] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, "Challenges of securing Internet of Things devices: A survey," Secur. Priv., vol. 1, no. 2, p. e20, Mar. 2018, doi: 10.1002/spy2.20.

[8] "Fractal resonator based frequency Reconfigurable Antenna with varying capacitive effect for wireless applications," Inf. MIDEM - J. Microelectron. Electron. Compon. Mater., vol. 51, no. 3, Dec. 2024, doi: 10.33180/InfMIDEM2025.104.

[9] G. Lackner, "A Comparison of Security in Wireless Network Standards with a Focus on Bluetooth, WiFi and WiMAX".

[10] H. El-Sofany, S. A. El-Seoud, O. H. Karam, and B. Bouallegue, "Using machine learning algorithms to enhance IoT system security," Sci. Rep., vol. 14, no. 1, p. 12077, May 2024, doi: 10.1038/s41598-024-62861-y.

[11] A. Shafique, A. Mehmood, M. Alawida, M. Elhadef, and M. U. Rehman, "A fusion of machine learning and cryptography for fast data encryption through the encoding of high and moderate plaintext information blocks," Multimed. Tools Appl., vol. 84, no. 8, pp. 5349–5375, Apr. 2024, doi: 10.1007/s11042-024-18959-6.

[12] S. S. Chaeikar, M. Alizadeh, M. H. Tadayon, and A. Jolfaei, "An intelligent cryptographic key management model for secure communications in distributed industrial intelligent systems," Int. J. Intell. Syst., vol. 37, no. 12, pp. 10158–10171, Dec. 2022, doi: 10.1002/int.22435.

[13] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," J. Supercomput., vol. 75, no. 10, pp. 6663–6682, Oct. 2019, doi: 10.1007/s11227-019-02878-7.

[14] A. BashirAbugharsa, A. Samad Bin Hasan Basari, and H. Almangush, "A New Image Encryption Approach using the Integration of a Shifting Technique and the AES Algorithm," Int. J. Comput. Appl., vol. 42, no. 9, pp. 36–45, Mar. 2012, doi: 10.5120/5723-7785.

[15] Y. Jha, K. Kaur, and C. Pradhan, "Improving image encryption using two-dimensional logistic map and AES," in 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, Tamilnadu, India: IEEE, Apr. 2016, pp. 0177–0180. doi: 10.1109/ICCSP.2016.7754116.

[16] M. S. Q. Khizrai and S. T. Bodkhe, "Image Encryption using Different Techniques for High Security Transmission over a Network," vol. 2, no. 4, 2014.

[17] A. H. Mohsen and S. H. Shaker, "Images encryption using symmetric encryption algorithm based on random keys generator," vol. 01, no. 08, 2016.

[18] S. Mohammed, S. M. K. Al-Alak, and H. A. Lafta, "ECC and AES Based Hybrid Security Protocol for Wireless Sensor Networks".

[19] S. N. Hussein and S. M. Al-Alak, "Secret Keys Extraction Using Light Weight Schemes for Data Ciphering," J. Phys. Conf. Ser., vol. 1999, no. 1, p. 012114, Sep. 2021, doi: 10.1088/1742-6596/1999/1/012114.

[20] P. Ji, H. Ma, Q. Ma, and X. Chen, "A Novel Method to Generate Pseudo-Random Sequence based on GAN".

[21] S. Park, K. Kim, K. Kim, and C. Nam, "Dynamical Pseudo-Random Number Generator Using Reinforcement Learning," Appl. Sci., vol. 12, no. 7, p. 3377, Mar. 2022, doi: 10.3390/app12073377.

[22] Y. Ding, F. Tan, Z. Qin, M. Cao, K.-K. R. Choo, and Z. Qin, "DeepKeyGen: A Deep Learning-based Stream Cipher Generator for Medical Image Encryption and Decryption," Dec. 21, 2020, arXiv: arXiv:2012.11097. doi: 10.48550/arXiv.2012.11097.

[23] V. Desai, R. Patil, and D. Rao, "Using Layer Recurrent Neural Network to Generate Pseudo Random Number Sequences," vol. 9, no. 2, 2012.

[24] V. Pachghare, Cryptography and information security. PHI Learning Pvt. Ltd., 2019.

[25] Y. F. M. Samsudeen, "Cryptography in Cybersecurity".

[26] POOJA BHATT and RACHNA NAVALAKHE, "REVIEW PAPER ON SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHIC ALGORITHMS," Jan. 2025, doi: 10.5281/ZENODO.14724450.

[27] M. Botta, M. Simek, and N. Mitton, "Comparison of hardware and software based encryption for secure communication in wireless sensor networks," in 2013 36th International Conference on Telecommunications and Signal Processing (TSP), Rome, Italy: IEEE, Jul. 2013, pp. 6–10. doi: 10.1109/TSP.2013.6613880.

[28] K. Sasikumar and S. Nagarajan, "Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing," IEEE Access, vol. 12, pp. 52325–52351, 2024, doi: 10.1109/ACCESS.2024.3385449.

[29] A. S. D. Alluhaidan and P. Prabu, "End-to-End Encryption in Resource-Constrained IoT Device," IEEE Access, vol. 11, pp. 70040–70051, 2023, doi: 10.1109/ACCESS.2023.3292829.

[30] J. Cao and J. Gao, "Research on Secure Transmission of Communication Data in Wireless Network Space: Encryption by an Improved AES Algorithm".

[31] A. M. Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," 2017.

[32] I. Goodfellow et al., "Generative adversarial networks," Commun. ACM, vol. 63, no. 11, pp. 139–144, Oct. 2020, doi: 10.1145/3422622.

[33] A. N. E. Wulandari, A. Ma'arif, W. A. Salah, and U. A. Dahlan, "Understanding Generative Adversarial Networks (GANs): A Review".

[34] L. Yuan, Y. Ma, and Y. Liu, "Protein secondary structure prediction based on Wasserstein generative adversarial networks and temporal convolutional networks with convolutional block attention modules," Math. Biosci. Eng., vol. 20, no. 2, pp. 2203–2218, 2022, doi: 10.3934/mbe.2023102.

[35] Z. Wang, Q. She, and T. E. Ward, "Generative Adversarial Networks in Computer Vision: A Survey and Taxonomy," Dec. 29, 2020, arXiv: arXiv:1906.01529. doi: 10.48550/arXiv.1906.01529.

The International Journal of Engineering Sciences
https://international-journal-of-engineering-sciences.jo
Vol. 2, No. 1, 2025, pp. 1-8
ISSN 3104-8897

[36] J. Gui, Z. Sun, Y. Wen, D. Tao, and J. Ye, "A Review on Generative Adversarial Networks: Algorithms, Theory, and Applications," Jan. 20, 2020, arXiv: arXiv:2001.06937. doi: 10.48550/arXiv.2001.06937.

[37] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing," Opt. Laser Technol., vol. 82, pp. 121–133, Aug. 2016, doi: 10.1016/j.optlastec.2016.02.018.

[38] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, 1949.

[39] M. A. Fadhil Al-Husainy, "A novel image encryption algorithm based on the extracted map of overlapping paths from the secret key," RAIRO-Theor. Inform. Appl.-Inform. Théorique Appl., vol. 50, no. 3, pp. 241–249, 2016.

[40] M. K. Hussein, K. R. Hassan, and H. M. Al-Mashhadi, "The quality of image encryption techniques by reasoned logic," TELKOMNIKA Telecommun. Comput. Electron. Control, vol. 18, no. 6, p. 2992, Dec. 2020, doi: 10.12928/telkomnika.v18i6.14340.

[41] "Image Encryption with The Cross Diffusion of Two Chaotic Maps," KSII Trans. Internet Inf. Syst., vol. 13, no. 2, Feb. 2019, doi: 10.3837/tiis.2019.02.031.

[42] M. J. Rostami, A. Shahba, S. Saryazdi, and H. Nezamabadi-pour, "A novel parallel image encryption with chaotic windows based on logistic map," Comput. Electr. Eng., vol. 62, pp. 384–400, 2017.