

Exploring Generative Adversarial Networks for Secure Data Encryption and Future Directions in Communication Systems

Ranjith Bhat^{1,2}  and Raghu Nanjundegowda³ 

¹Dept of Robotics and AI Engineering, NMAM Institute of Technology, NITTE (Deemed to be University) Nitte, India

²Dept of Electronics and Communication JAIN (Deemed to be University) Bengaluru, India

³Dept of Electrical and Electronics Engineering JAIN (Deemed to be University) Bengaluru, India

Keywords: Artificial Intelligence, Generative Adversarial Network (GANs), Image Encryption, Multilevel GAN.


Abstract: The rapid advancements in communication systems and the proliferation of digital technologies have underscored the critical need for robust and adaptive encryption methods to safeguard data integrity, confidentiality, and authenticity. Traditional cryptographic techniques, while effective, face challenges in the wake of evolving cyber threats and emerging technologies such as quantum computing. This paper explores the transformative potential of Generative Adversarial Networks (GANs) in secure data encryption and communication systems. By leveraging the dynamic architecture of GANs, which consists of a generator and a discriminator operating in an adversarial framework, novel encryption methodologies are developed. These methodologies address limitations in traditional encryption by introducing non-linear, adaptive encryption schemes resistant to reverse engineering and capable of generating dynamic encryption keys. The paper further investigates the integration of GANs into modern communication paradigms, including quantum communication, blockchain networks, and IoT systems. Additionally, it highlights the challenges in adopting GAN-based encryption, including training instability, scalability, and adversarial vulnerabilities, while proposing solutions to overcome these issues. Through experimental validation, the study demonstrates the superior security and efficiency of GAN-based encryption systems, offering a scalable and intelligent approach to securing data in an increasingly complex digital landscape.


1 INTRODUCTION

The rapid advancement of communication systems and the proliferation of digital technologies have fundamentally reshaped the way data is exchanged, stored, and processed (Goodfellow, 2014). From personal communications to global financial systems, the reliance on secure data transmission has become an indispensable requirement in ensuring the integrity, confidentiality, and authenticity of information (Cao, 2020). However, the ever-increasing sophistication of cyberattacks and data breaches has exposed the vulnerabilities in existing encryption methodologies, demanding more robust and adaptive solutions for securing communication systems. Traditional cryptographic techniques such as symmetric and asymmetric encryption methods have been the cornerstone of secure communication

for decades. While these methods are effective against many contemporary threats, the rise of quantum computing and other disruptive technologies presents significant challenges to their long-term viability (Wang, 2018). As attackers develop more advanced techniques, it becomes imperative to explore innovative and intelligent approaches to encryption that can not only resist these threats but also adapt to evolving attack vectors in real time. This has led researchers to investigate the potential of emerging technologies, such as artificial intelligence (AI) and machine learning (ML), to revolutionize secure communication (Singh, 2023).

Generative Adversarial Networks (GANs) represent a significant advancement in artificial intelligence and machine learning, functioning as an effective mechanism for the generation of realistic synthetic data, including images, videos, and text.

^a  <https://orcid.org/0009-0000-6149-1243>

^b  <https://orcid.org/0000-0002-2091-8922>

Since their introduction by Ian Goodfellow and colleagues in 2014, Generative Adversarial Networks (GANs) have been extensively utilized in various applications, such as image synthesis, data augmentation, and anomaly detection, among others (Li, 2020). Generative Adversarial Networks (GANs) fundamentally comprise two neural networks: a generator and a discriminator. These networks engage in a competitive process characterized as a zero-sum game, as illustrated in Fig. 1. The adversarial dynamic enables GANs to learn intricate data distributions and produce outputs that cannot be differentiated from real data (Zahmoul, 2016).

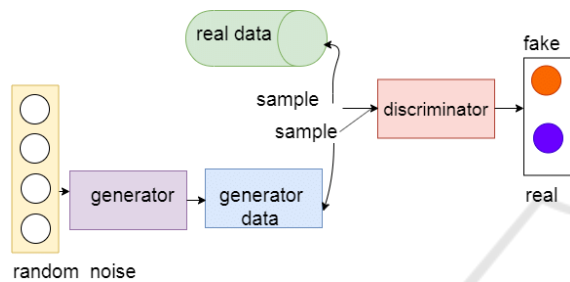


Figure 1: A typical GAN architecture.

The training set consists of the set of real images illustrated in the figure, while random noise is provided to the Generator to initiate the training process. Both the neural networks are trained further and updated as per the loss function available through the back propagation. In the context of secure data encryption, GANs offer an intriguing paradigm shift (Li and Li, 2019). Unlike traditional encryption methods that rely on deterministic algorithms, GANs can generate highly complex and adaptive encryption schemes that are inherently resistant to reverse engineering. By leveraging their ability to learn and adapt, GANs can create non-linear, dynamic encryption keys that are extremely difficult for adversaries to decipher, even with access to advanced computational resources. Additionally, GANs can be utilized to detect and counteract security threats in real time, further enhancing the resilience of communication systems (Bhat and Nanjundegowda, 2025).

This paper explores the potential of GANs in transforming secure data encryption and communication systems. We propose a novel framework for leveraging GANs to develop adaptive encryption algorithms that can address the limitations of traditional methods while offering enhanced protection against emerging threats. Furthermore, we investigate the integration of GANs into futuristic communication paradigms, such as quantum

communication systems, blockchain-based networks, and the Internet of Things (IoT), where the need for innovative security solutions is paramount (Zhang, 2020).

In addition to discussing the strengths and potential of GAN-based encryption, we also examine the challenges and limitations associated with their adoption. Issues such as computational complexity, scalability, and the risk of adversarial attacks on GANs themselves are critical factors that must be addressed to realize their full potential (Zhang, 2018). Furthermore, ethical considerations and regulatory frameworks for deploying AI-driven encryption techniques will be explored, ensuring that these technologies are implemented responsibly and securely (Zhao, 2022).

The structure of this paper is as follows: Section 2 provides a comprehensive overview of GANs, their architecture, and key principles. Section 3 delves into the application of GANs for secure data encryption, outlining proposed methodologies and use cases. Section 4 discusses the challenges, limitations, and potential risks associated with GAN-based encryption systems. Section 5 highlights future research directions and opportunities for advancing GANs in the context of secure communication. Finally, Section 6 concludes the paper by summarizing key findings and emphasizing the transformative potential of GANs in redefining secure communication systems.

Through this research, we aim to bridge the gap between cutting-edge AI technologies and the pressing need for advanced encryption mechanisms, providing a foundation for future innovations in secure communication (Li, 2019). By harnessing the power of GANs, we envision a new era of adaptive, resilient, and intelligent communication systems capable of withstanding the challenges of an increasingly complex digital landscape (Bhat, 2025).

2 RELATED WORKS

A neural network was designed for impulsive coordination within the reaction-diffusion mechanism, effectively modelling the dynamic behaviours of these systems (Chen, 2016). This method was later utilized for image encryption purposes. Chaotic systems demonstrate notable cryptographic potential, particularly in the context of image cryptosystems, providing robust security features against various traditional attacks, such as plaintext attacks. The neural network described was later employed in image cryptosystems. A scheme

that combines chaotic systems with neural networks, resulting in a solution that exhibits improved security and decreased complexity compared to previous methods (Dridi, 2016). An image encryption scheme utilizing a stacked autoencoder network to generate chaotic sequences. The scheme exhibited significant efficiency, attributable to the parallel computing capabilities of the stacked autoencoder and its resilience against conventional attacks (Hu, 2017). In a specific study, a new image steganography technique that avoided the embedding of messages within carrier images. The deep model demonstrated significant improvements in image security metrics, exhibited an effective extraction phase, and showed strong resilience against steganalysis algorithms (Hu, 2018).

An image encryption approach (Li, 2018) using a CNN trained on the CASIA iris dataset (Debiasi, 2015) to generate encryption keys. Iris characteristics were retrieved and encoded using RS error-correcting codes. The encoded vector was used to XOR-encrypt plain images. An encryption keys with a Montgomery County chest X-ray dataset-trained GAN (Ding, 2020). This updated system has a larger key space, better pseudo-randomness, resilience to typical image processing assaults, and higher modification sensitivity (Jaeger, 2014). A scheme utilizing a deep neural network that removed the requirement for pre-shared keys between systems (Jin, 2020). The system dynamically generated and utilized encryption keys, resulting in enhanced overall security. A DNN-based image encryption scheme that employs the SIPI image dataset. This scheme integrates chaotic maps for the encryption process, ensuring the preservation of image quality (Manivath, 2020).

An encryption method that employs multiple chaotic sequences generated from sensitive keys, which were derived by training a convolutional neural network (CNN) on the ImageNet database (Erkan, 2022). The initial conditions for encryption in the hyperchaotic logistic map were determined using parameters produced by the network. A two-layer deep neural network aimed at classifying silica aerogel (SA) in the context of physical unclonable functions (Fratalocchi, 2020). The chaotic behavior of SA was employed to produce cryptographic keys, yielding random key sequences for various input conditions. We strongly encourage authors to use this document for the preparation of the camera-ready. Please follow the instructions closely in order to make the volume look as uniform as possible (Moore and Lopes, 1999).

An image encryption scheme that employs a Cycle-GAN architecture. The network was trained

using a dataset consisting of both plain and cipher satellite images. This approach utilized double random phase encoding to achieve image encryption (Li, 2021). An alternative scheme utilizing Cycle-GAN, which was trained on a chest X-ray dataset (Ding, 2021). This scheme not only executed encryption-decryption tasks but also detected specific objects within the cipher images. The flaws in prior techniques to establish a foundation for an improved avalanche impact (Bao, 2021). A sophisticated framework was introduced that integrates a diffusion mechanism. The neural network, trained on satellite image datasets from Google Maps, demonstrated enhanced efficiency; nonetheless, it displayed inadequate performance in the decryption process (Baluja, 2017).

Cycle-GAN networks are extensively utilized in encryption and decryption operations inside deep learning-based image encryption frameworks, including picture steganography, showcasing their versatility in modern cryptographic applications. An experimental results reveal that CryptoGAN achieves high levels of randomness and unpredictability, essential for secure encryption, and provides strong resistance to cryptanalysis (Bhat, 2024). This study highlights the potential of CryptoGAN to revolutionize image security by combining traditional cryptography with advanced machine learning techniques. At addressing limitations in traditional encryption methods like AES and chaotic encryption, CryptoGAN combines U-Net as the generator and PatchGAN as the discriminator to encrypt and decrypt images while maintaining high visual fidelity and robust security (Bhat, 2024). Trained on a dataset of 2000 butterfly images, CryptoGAN ensures structural similarity, high entropy, and low pixel correlation, effectively resisting cryptanalysis and statistical attacks. The model achieves superior performance compared to existing methods, with high SSIM and PSNR values.

3 CHALLENGES

Advanced GAN-based models have received significant focus in the field of cybersecurity. Nonetheless, the implementation of these methods in encryption and decryption presents certain challenges. This section examines the primary challenges faced in utilizing GANs for cybersecurity, with a focus on protecting digital assets and the effective implementation of these models. The use of GANs in encryption and decryption faces several technical challenges, including training instability

and mode collapse, which may adversely affect the performance and reliability of these models. The integration of GANs into existing security frameworks presents a significant challenge, necessitating precise alignment to guarantee seamless functionality and scalability.

3.1 Cryptographic Challenges

Despite their potential, GANs face notable challenges when applied to image data encryption. One significant issue is the inconsistency and limited diversity in the quality of generated image data. This limitation can undermine the effectiveness of using GAN-generated images in testing encryption algorithms, where reliability and diversity are essential. Additionally, GAN training can be unstable, often leading to difficulties in achieving convergence. This instability not only complicates the optimization process but also impacts the evaluation of the model's performance in encryption-related tasks.

To address these challenges, a new symmetric encryption framework called Adversarial Neural Cryptography (ANC) has been introduced, specifically designed for image data. ANC integrates GANs into its structure to enhance encryption capabilities and provide robust security against chosen-ciphertext attacks (CCA). The ANC system models secure communication between two entities, Alice and Bob, who exchange encrypted image data using a shared key K . Meanwhile, Eve, a passive attacker, attempts to decode the plaintext image P by analysing the ciphertext C .

In developing the ANC system, particular focus is given to resisting CCA attacks. The system employs a multi-layer encryption strategy coupled with a sophisticated key exchange mechanism to minimize the statistical correlation between plaintext images and their corresponding ciphertext. This approach significantly increases the difficulty for attackers attempting to breach the system. Additionally, the GAN's generator is utilized to introduce higher levels of randomness and unpredictability to the ciphertext images, further bolstering the system's resilience to CCA attacks.

Experimental findings confirm the effectiveness of ANC in mitigating CCA threats. By leveraging the GAN's ability to enhance the randomness in ciphertext, the feasibility of attackers conducting statistical analysis is greatly reduced. Fig. 2 illustrates the symmetric encryption and decryption model used in ANC for image data using 2 parties Alice and Bob using the same symmetric Key which is both used for

Encryption and Decryption. The experiments also evaluate ANC's performance in simulated attack scenarios, highlighting its robustness in protecting encrypted image communication and ensuring secure exchanges. Overall, while challenges such as training instability and variability in data quality exist, the integration of GANs into cryptographic systems like ANC demonstrates their transformative potential. By addressing these limitations, ANC effectively harnesses GANs to improve both the efficiency and security of encryption methodologies for image data, paving the way for more advanced and secure cryptographic systems.

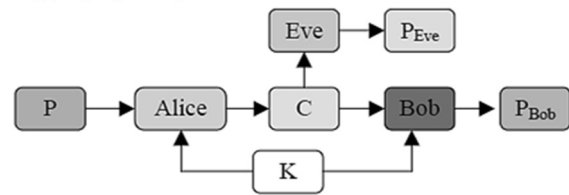


Figure 2: Symmetric Encryption scheme used by two parties

3.2 Cybersecurity Challenges

This section highlights key challenges in cybersecurity, particularly in addressing adversarial attacks and implementing advanced techniques like GANs and federated learning.

3.2.1 Adversarial Attacks and Adversarial Example Generation

Challenges posed by adversarial evasion attacks, where altered input samples deceive classifiers, compromising botnet detection accuracy (Randhawa, 2021). While efforts to improve recall rates and address dataset imbalance using GANs for synthetic oversampling show promise, challenges remain in generating diverse, high-quality datasets and keeping up with evolving attack methods. Further, modern botnets require updated traffic features for effective differentiation, emphasizing the need for continuous research.

The emergence of Adversarial Examples (AEs) in cybersecurity. AEs are malicious perturbations that mislead classifiers, posing threats to machine learning (ML)-based systems (Zhang, 2020). While most research on AEs focuses on computer vision, their impact on cybersecurity systems remains underexplored, underscoring the need for robust ML models that can withstand adversarial attacks.

Challenges in countering adversarial attacks, where malicious samples deceive both humans and ML systems (Schneider, 2023). These attacks exploit

vulnerabilities in malware classifiers and pose significant risks to cybersecurity (Lucas, 2023). Defence strategies, like adversarial training and frameworks such as Défense-GAN, aim to enhance robustness against such attacks, but their effectiveness varies across datasets and attack types (Laykaviriniyakul, 2023).

3.3 Network Security Challenges

The growing challenges in network security, driven by rapid technological advancements and an expanding number of internet users (Yang, 2022). The increase in network traffic, fuelled by the rise of 5G networks, and the emergence of threats like trojan horses, viruses, and phishing sites have made detecting and mitigating network threats more complex. This necessitates improved methods for proactive defence and network threat detection.

In a related study, (Das, 2022) emphasized the challenges posed by the dynamic nature of computer and mobile networks. Increasing nodes and traffic complicate anomaly detection and adaptation to modern attacks. Privacy concerns in intrusion detection systems and challenges like coordinating updates in large-scale networks and preventing model tampering were addressed using federated learning. This approach enables secure sharing of encrypted models while preserving data privacy.

The vulnerabilities arising from diversified access points in 5G and distributed networks, which have expanded the attack surface (Park, 2022). The increasing frequency and sophistication of cyberattacks make detection and prevention more difficult, emphasizing the need for enhanced intrusion detection systems to safeguard networks. Limitations in current botnet detection methods, noting their inability to fully capture the evolving and sophisticated behaviours of botnets (Yin, 2018). These adaptive threats, which leverage advanced technologies to evade detection, present a significant challenge, underscoring the need for more comprehensive network flow analysis.

leveraging the unique architecture of GANs, which consists of a generator and a discriminator. These two neural networks operate in a competitive framework where the generator produces encrypted versions of images, and the discriminator evaluates the authenticity or quality of these outputs. This adversarial process allows the generator to learn intricate transformations that obscure the content of the original image while maintaining a structured framework for decryption.

It is assumed that both the generator (G) and discriminator (D) models possess sufficient capacity to handle the required tasks. When the generator's data distribution $p_g(x)$ aligns perfectly with the real data distribution $p_{data}(x)$, the GAN model achieves a state of equilibrium. At this point, the discriminator D cannot distinguish between real and generated data, resulting in a classification accuracy of 50%. Here, $p_g(x)$ represents the distribution of data generated by the generator. Formally, for a specific generator G, the optimal discriminator D^* can be determined.

A commonly used approach in GANs is the hierarchical structure, which allows encrypted images to be generated step-by-step, gradually improving their resolution at each stage. This hierarchical architecture is particularly beneficial for applications that require high-quality outputs, such as image encryption. For instance, MultiLevelGAN utilizes this method to generate progressively detailed outputs, as depicted in Fig. 3. Compared to traditional encryption techniques, GANs demonstrate a significant advantage in terms of generation speed. By replacing the traditional sampling process with a generator, GANs eliminate the need for a lower bound to approximate likelihood, streamlining the generation process.

A critical component of the encryption process is the generation of secure and pseudo-random keys. GANs can be trained to generate such keys by learning from chaotic systems like logistic maps, which provide high randomness and unpredictability. The generator produces encryption keys that are inherently complex and difficult to decipher, ensuring the robustness of the encryption process.

4 SUGGESTED METHODOLOGIES FOR ENCRYPTION WITH GANS

Designing a robust image encryption scheme using Generative Adversarial Networks (GANs) involves

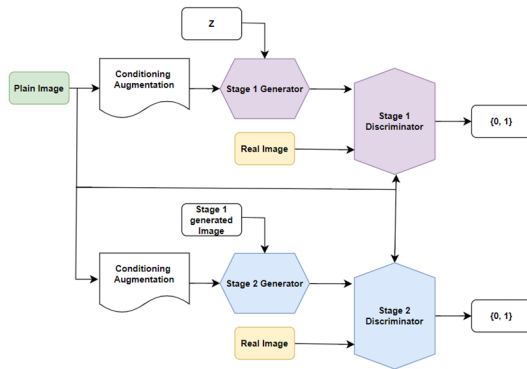


Figure 3: Architecture of MultiLevelGAN.

These keys form the foundation for encryption operations, including substitution, permutation, and diffusion, which collectively transform the original image into an unintelligible form. Substitution modifies the pixel values based on the generated key, permutation rearranges the pixel positions to disrupt spatial coherence, and diffusion ensures that small changes in the original image result in significant differences in the encrypted output.

The encryption process begins with training the GAN using a dataset of images, where the generator learns to encrypt the images, and the discriminator assesses the quality of encryption. The goal of training is for the generator to produce encrypted images that are indistinguishable from a target distribution, effectively confusing the discriminator. This iterative adversarial training ensures that the generator develops the capability to perform highly secure and adaptive encryption. The discriminator, in turn, becomes a robust evaluator of the encryption quality, pushing the generator to continually improve. Once the encryption process is established, the decryption mechanism reverses the transformations applied during encryption. Using the same key generated by the GAN, the encrypted image undergoes inverse diffusion, permutation, and substitution to reconstruct the original image. The decryption process is designed to be lossless, ensuring that the original image is retrieved without any degradation in quality. This reversibility is a critical aspect of the encryption scheme, as it ensures usability without compromising security.

The security of the GAN-based encryption scheme is rigorously analysed to confirm its robustness. Statistical analysis is performed on the encrypted images to verify the uniformity of pixel value distributions, indicating effective encryption. Key sensitivity analysis ensures that even slight variations in the key render the decryption process

ineffective, highlighting the system's dependency on the exact key for secure operations. Additionally, the scheme is subjected to various attacks, including brute force, differential, and statistical attacks, to evaluate its resilience. Studies have demonstrated that GAN-based encryption methods are highly resistant to such attacks, offering a robust framework for secure image transmission and storage.

Implementing a GAN-based encryption scheme requires careful consideration of computational resources and dataset quality. Training GANs is computationally intensive and demands substantial processing power. The quality and diversity of the training dataset significantly influence the GAN's ability to generate effective encryption keys. Furthermore, hyperparameters such as learning rates and network architectures must be carefully tuned to achieve optimal performance. Despite these challenges, GAN-based encryption provides a flexible and adaptive framework for securing images in a variety of applications.

In Figure 4, a Secure Transformation Network (STN) processes plaintext and keys by first converting them into angles using $f(b)$ as input to the neural network. The weight matrix multiplication in the adversarial encrypting network is then computed to generate the initial ciphertext. The final ciphertext is obtained by applying the inverse transformation $f^{-1}(a)$. Notably, all data handled by the STN are floating-point numbers, with ciphertext values constrained to the range $[0, 1]$.

Mathematically, the fully connected layer of the cipher set performs operations as described in Equation (1):

$$\begin{pmatrix} h_0 & h_1 & h_2 & \dots & h_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & \dots & a_{n-1} & a_n & \dots & h_{2n-1} \end{pmatrix} W \quad (1)$$

Here, W represents the unified weight matrix of all hidden and convolutional layers in the adversarial encrypting network.

$\begin{pmatrix} a_0 & \dots & a_{n-1} & a_n & \dots & a_{2n-1} \end{pmatrix}$ corresponds to the angles of the plaintext and key, while $\begin{pmatrix} h_0 & h_1 & h_2 & \dots & h_{n-1} \end{pmatrix}$ represents the network's output variables.

In the rest of the experiment, the cipher set is expressed mathematically as shown in Equation (2): This section must be in two columns.

$$C = \xi(W, PI, KI) \quad (2)$$

where P , K , and C denote the plaintext, key, and ciphertext as n -bit vectors, respectively.

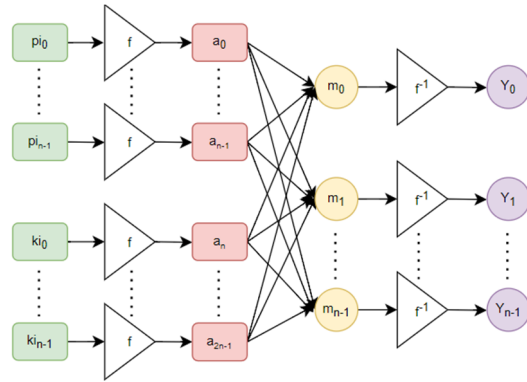


Figure 4: Neural Network of MultiLevelGAN

This idea presents an analysis of the encryption structure, algorithm functionality, and security performance of the Adversarial Neural Cryptography (ANC) system, specifically when applied to image data. While ANC has shown potential, previous research highlights vulnerabilities when ANC is combined with multi-layer neural networks for computer communication systems. Specifically, it has been observed that such systems can be cracked by adversarial neural networks through training.

To address these challenges, this study proposes an enhanced adversarial encryption algorithm called CCA-ANC, tailored for image data. The core idea behind CCA-ANC is to simulate a stronger attacker with greater cracking capabilities, thereby forcing the sender and legitimate receiver to adopt a more robust encryption system. This approach results in a highly secure and resilient encryption method.

4.1 Concept of CCA-ANC for Image Data

The Chosen-Ciphertext Attack (CCA) technique in CCA-ANC allows an attacker to select a sequence of ciphertexts and analyse the corresponding plaintext or key information. This method is particularly effective for evaluating the security of the ANC algorithm. By applying CCA, potential weaknesses in the encryption mechanism can be identified and addressed, leading to algorithm improvements. For image data, this technique ensures the encryption system can withstand sophisticated cryptographic attacks and enhances the system's overall security and reliability in real-world applications.

4.2 Continuous XOR for Image Encryption

One of the novel contributions of this experiment is the extension of the XOR operation to a continuous space, optimized for image encryption. Traditional XOR, commonly used in cryptography, is adapted using a unit circle representation. The experiment maps binary values (0 and 1) to corresponding angles (0 and π), enabling a continuous transformation. The resulting XOR operation becomes the sum of two angles, making it more suitable for continuous data, such as image pixels.

The mapping of bit positions to angles is defined by the following equations:

1. Mapping bit position to angle:

$$f(b) = \arccos(1 - 2b) \quad (3)$$

Here in (3), $f(b)$ represents the conversion of bit position b to an angle.

2. Inverse mapping of angle to continuous bits:

$$f^{-1}(a) = \frac{1 - \cos(a)}{2} \quad (4)$$

In (4) inverse function transforms the angle back to its original bit representation.

This continuous XOR operation enables the encryption of image data in a floating-point space, making the process more flexible and secure for high-resolution and complex image datasets.

4.3 Secure Transformation Network (STN)

To verify the security of the encryption process, a Secure Transformation Network (STN) is introduced. The STN, as shown in Figure 4, is designed to evaluate the robustness of the encryption mechanism by learning and detecting potential vulnerabilities.

The structure of STN is as follows:

Input Conversion: The plaintext and keys are transformed into angles using the $f(b)$ mapping, converting bits into angles for input into the neural network.

Adversarial Encryption: A weight matrix multiplication is performed within the adversarial encryption network to generate the initial ciphertext.

The STN processes all data as floating-point numbers, with the resulting ciphertext values constrained to the range $[0, 1]$. This ensures precision and adaptability when encrypting and decrypting image data.

5 CONCLUSIONS AND FUTURE SCOPES

The potential of GAN-based encryption extends beyond traditional use cases, with opportunities for integration into real-time systems and cross-modal encryption tasks. Future research can focus on developing specialized GAN architectures tailored for encryption, optimizing real-time performance, and expanding the scope of encryption to other data modalities such as video and audio. By addressing these directions, GANs can revolutionize secure communication systems, ensuring the confidentiality and integrity of data in an increasingly interconnected digital world. The adaptability and learning capabilities of GANs make them a promising avenue for advancing encryption methodologies and overcoming the challenges posed by emerging cyber threats.

REFERENCES

- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial nets. *Advances in neural information processing systems*, 27.
- Cao, W., Mao, Y., & Zhou, Y. (2020). Designing a 2D infinite collapse map for image encryption. *Signal Processing*, 171, 107457.
- Wang, X., Zhu, X., & Zhang, Y. (2018). An image encryption algorithm based on Josephus traversing and mixed chaotic map. *IEEE Access*, 6, 23733-23746.
- Singh, M., Baranwal, N., Singh, K. N., & Singh, A. K. (2023). Using GAN-based encryption to secure digital images with reconstruction through customized super resolution network. *IEEE Transactions on Consumer Electronics*, 70(1), 3977-3984.
- Li, Q., Wang, X., Wang, X., Ma, B., Wang, C., Xian, Y., & Shi, Y. (2020). A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks. *IEEE Access*, 8, 168166-168176.
- Zahmoul, R., & Zaied, M. (2016, October). Toward new family beta maps for chaotic image encryption. In 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 004052-004057). IEEE.
- Zhang, Y., Jia, R., Pei, H., Wang, W., Li, B., & Song, D. (2020). The secret revealer: Generative model-inversion attacks against deep neural networks. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 253-261).
- Zhang, R., Isola, P., Efros, A. A., Shechtman, E., & Wang, O. (2018). The unreasonable effectiveness of deep features as a perceptual metric. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 586-595).
- Zhao, D., Zhu, X., Liu, B., Ren, J., Zhu, X., Mao, Y., ... & Ullah, R. (2022). High-security and low-complexity OCDM transmission scheme based on GAN enhanced chaotic encryption. *Optics Express*, 30(19), 34898-34907.
- Li, X., & Li, X. (2019, July). A novel block image encryption algorithm based on DNA dynamic encoding and chaotic system. In 2019 IEEE 4th international conference on signal and image processing (ICSIP) (pp. 901-906). IEEE.
- Bhat, R., & Nanjundegowda, R. (2025). A Review on Comparative Analysis of Generative Adversarial Networks' Architectures and Applications. *Journal of Robotics and Control (JRC)*, 6(1), 53-64.
- Chen, W. H., Luo, S., & Zheng, W. X. (2016). Impulsive synchronization of reaction-diffusion neural networks with mixed delays and its application to image encryption. *IEEE transactions on neural networks and learning systems*, 27(12), 2696-2710.
- Dridi, M., Hajjaji, M. A., Bouallegue, B., & Mtibaa, A. (2016). Cryptography of medical images based on a combination between chaotic and neural network. *IET Image Processing*, 10(11), 830-839.
- Hu, F., Wang, J., Xu, X., Pu, C., & Peng, T. (2017). Batch image encryption using generated deep features based on stacked autoencoder network. *Mathematical Problems in Engineering*, 2017(1), 3675459.
- Hu, D., Wang, L., Jiang, W., Zheng, S., & Li, B. (2018). A novel image steganography method via deep convolutional generative adversarial networks. *IEEE access*, 6, 38303-38314.
- Li, X., Jiang, Y., Chen, M., & Li, F. (2018). Research on iris image encryption based on deep learning. *EURASIP Journal on Image and Video Processing*, 2018, 1-10.
- Debiasi, L., & Uhl, A. (2015, March). Techniques for a forensic analysis of the casia-iris v4 database. In 3rd International Workshop on Biometrics and Forensics (IWBF 2015) (pp. 1-6). IEEE.
- Ding, Y., Wu, G., Chen, D., Zhang, N., Gong, L., Cao, M., & Qin, Z. (2020). DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. *IEEE Internet of Things Journal*, 8(3), 1504-1518.
- Jaeger, S., Candemir, S., Antani, S., Wang, Y. X. J., Lu, P. X., & Thoma, G. (2014). Two public chest X-ray datasets for computer-aided screening of pulmonary diseases. *Quantitative imaging in medicine and surgery*, 4(6), 475.
- Jin, J., & Kim, K. (2020). 3D CUBE algorithm for the key generation method: Applying deep neural network learning-based. *IEEE Access*, 8, 33689-33702.
- Maniyath, S. R., & Thanikaiselvan, V. (2020). An efficient image encryption using deep neural network and chaotic map. *Microprocessors and Microsystems*, 77, 103134.
- Erkan, U., Toktas, A., Enginoğlu, S., Akbacak, E., & Thanh, D. N. (2022). An image encryption scheme based on chaotic logarithmic map and key generation

- using deep CNN. *Multimedia Tools and Applications*, 81(5), 7365-7391.
- Fratalocchi, A., Fleming, A., Conti, C., & Di Falco, A. (2020). NIST-certified secure key generation via deep learning of physical unclonable functions in silica aerogels. *Nanophotonics*, 10(1), 457-464.
- Li, J., Zhou, J., & Di, X. (2021). A learning optical image encryption scheme based on CycleGAN. *J. Jilin Univ. (Eng. Technol. Ed.)*, 51(3), 1060-1066.
- Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K. K. R., & Qin, Z. (2021). DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption. *IEEE Transactions on Neural Networks and Learning Systems*, 33(9), 4915-4929.
- Bao, Z., & Xue, R. (2021). Research on the avalanche effect of image encryption based on the Cycle-GAN. *Applied Optics*, 60(18), 5320-5334.
- Bao, Z., Xue, R., & Jin, Y. (2021). Image scrambling adversarial autoencoder based on the asymmetric encryption. *Multimedia Tools and Applications*, 80(18), 28265-28301.
- Baluja, S. (2017). Hiding images in plain sight: Deep steganography. *Advances in neural information processing systems*, 30.
- Bhat, R., & Nanjundegowda, R. (2024). CryptoGAN: a new frontier in generative adversarial network-driven image encryption. *Int J Artif Intell*, 13(4), 4813-4821.
- Bhat, R., & Nanjundegowda, R. (2024). Comparative Analysis of CryptoGAN: Evaluating Quality Metrics and Security in GAN-based Image Encryption. *Journal of Robotics and Control (JRC)*, 5(5), 1557-1569.
- Randhawa, R. H., Aslam, N., Alauthman, M., Rafiq, H., & Comeau, F. (2021). Security hardening of botnet detectors using generative adversarial networks. *IEEE Access*, 9, 78276-78292.
- Zhang, S., Xie, X., & Xu, Y. (2020). A brute-force black-box method to attack machine learning-based systems in cybersecurity. *IEEE Access*, 8, 128250-128263.
- Schneider, J., & Apruzzese, G. (2023). Dual adversarial attacks: Fooling humans and classifiers. *Journal of Information Security and Applications*, 75, 103502.
- Lucas, K., Pai, S., Lin, W., Bauer, L., Reiter, M. K., & Sharif, M. (2023). Adversarial training for {Raw-Binary} malware classifiers. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 1163-1180).
- Laykaviriyakul, P., & Phaisangittisagul, E. (2023). Collaborative Defense-GAN for protecting adversarial attacks on classification system. *Expert Systems with Applications*, 214, 118957.
- Yang, Y., Yao, C., Yang, J., & Yin, K. (2022). A network security situation element extraction method based on conditional generative adversarial network and transformer. *IEEE Access*, 10, 107416-107430.
- Das, S. (2022). FGAN: Federated generative adversarial networks for anomaly detection in network traffic. *arXiv preprint arXiv:2203.11106*.
- Park, C., Lee, J., Kim, Y., Park, J. G., Kim, H., & Hong, D. (2022). An enhanced AI-based network intrusion detection system using generative adversarial networks. *IEEE Internet of Things Journal*, 10(3), 2330-2345.
- Yin, C., Zhu, Y., Liu, S., Fei, J., & Zhang, H. (2018, May). An enhancing framework for botnet detection using generative adversarial networks. In *2018 International Conference on Artificial Intelligence and Big Data (ICAIBD)* (pp. 228-234). IEEE.