Mesopotamian journal of Computer Science
Vol. **(2025)**, 2025, **pp**. 371–370
DOI: https://doi.org/10.58496/MJCSC/2025/024 ;ISSN: 2958-6631
https://mesopotamian.press/journals/index.php/cs

Research Article

DGEN: A Dynamic Generative Encryption Network for Adaptive and Secure Image Processing

Mohammed Rajih Jassim[1], Qusay M. Salih [2], Ghada Al-Kateb [3] , *,

[1] *College of Production Engineering and Metallurgy, University of Technology, Iraq*

[2] *Department of Computer Engineering, College of Engineering, University of Baghdad, Iraq*

[3] *Department of Mobile Computing and Communication, Faculty of Engineering, University of Information Technology and Communication, Iraq*

ARTICLEINFO

Article History

Received 5 Aug 2025
Revised 06 Sep 2025
Accepted 02 Oct 2025
Published 05 Oct 2025

Keywords

Generative Encryption
Adaptive Security
Neural Networks
Lightweight Cryptography
Image Processing

ABSTRACT

Cyber-attacks keep growing. Because of that, we need stronger ways to protect pictures. This paper talks about DGEN, a Dynamic Generative Encryption Network. It mixes Generative Adversarial Networks with a key system that can change with context. The method may potentially mean it can adjust itself when new threats appear, instead of a fixed lock like AES. It tries to block brute-force, statistical tricks, or quantum attacks. The design adds randomness, uses learning, and makes keys that depend on each image. That should give very good security, some flexibility, and keep compute cost low. Tests still ran on several public image sets. Results show DGEN beats AES, chaos tricks, and other GAN ideas. Entropy reached 7.99 bits per pixel, correlation dropped 0.002, and the avalanche effect was 95.4 percent. Encrypting a surveillance frame took 7.5 ms, while the picture quality stayed high, with PSNR 39.7 dB and SSIM 99.2. These numbers suggest the tool can still work in real time and scale up significantly. The study also looks at how DGEN could fit with quantum computers and federated learning, hinting it might be a very big step forward for safe image handling.

1. INTRODUCTION

Protecting image data in today's fast-changing digital communication scene may be crucial specially since data-heavy apps keep expanding rapidly, importance appears undeniable true. [1]. The rising sophistication of cyber threats, combined with the proliferation of visual content in essential sectors such as healthcare, defense, and Internet of Things (IoT) networks, necessitates encryption mechanisms that are not only strong but also adaptable and future ready [2]. Although traditional cryptographic methods remain valuable in several contexts, their limited scalability and rigidity often render them insufficient in confronting dynamic threats and the heterogeneity of modern visual data [3,4]. Recent AI strides, especially in generative models, seem to shake many fields. GANs, for instance, may go beyond picture making to help restore old photos or improve video quality. Yet, their limits raise questions about reliability in real life contexts [5]. Nevertheless, their applicability to cryptographic systems remains largely underexplored [6]. This research addresses this gap by proposing the **Dynamic Generative Encryption Network (DGEN)**, a novel paradigm that leverages the adaptive generative power of GANs to transform image encryption. Unlike conventional methods that rely on fixed and predictable algorithms, DGEN employs artificial intelligence to produce secure, context-aware, and highly unpredictable encryption schemes tailored to each image.

The main contributions of this paper are as follows:

1. **A Dynamic Encryption Framework**: First, the work introduces DGEN, a kind of dynamic encryption that appears to use GANs to tweak protection for each image in real time.
2. **Enhanced Security Features**: Second, it adds an entropy-boosted layer, which may give the cipher more randomness and could help against even future quantum attacks.

*Corresponding author. Email: ghada.emad@uoitc.edu.iq

3. **Efficiency and Scalability**: Third, experiments suggest DGEN works fast enough for many data types, from IoT sensors to live video feeds, and it's grown.
4. **Practical Relevance**: Finally, the authors show possible uses such as keeping medical scans safe, helping autonomous cars stay secure, and fitting into new blockchain login systems.By addressing the shortcomings of existing encryption techniques and integrating state-of-the-art AI methodologies, this study establishes a new benchmark in image security. The subsequent sections provide a detailed description of the DGEN framework, experimental evaluation, and its implications for advancing secure image processing.

2. RELATED WORK

Al-Khalisy et al. [7] proposed QIULEA, a quantum-inspired ultra-lightweight IoT encryption algorithm. Their research showed that when compared to traditional methods, QIULEA offered an improved processing speed, a remarkably reduced memory footprint, and an enhanced speed of computing. This study emphasizes how well quantum physical principles might work up against classical principles when optimizing cryptosystems for not just powerful computing environments but also for resource-constrained "edge" devices. Another notable contribution is the work of Jewani et al. [8], who investigated the application of Generative Adversarial Networks (GANs) in cybersecurity. GANs appear to boost cybersecurity by creating believable attack mock-ups, which likely help intrusion detection work better in practice. This gives a useful base for forward-thinking threat modeling in IoT security overall.

2.1 Lightweight Encryption and Post-Quantum Cryptography

A study on SIMECK-T [9] introduces a lightweight encryption scheme that integrates the SIMECK and TEA algorithms. This hybrid design strengthens security while maintaining minimal computational overhead, thereby making it particularly suitable for resource-constrained IoT environments. The work highlights the critical need to strike a balance between robust security guarantees and energy efficiency in embedded systems. Within the scope of post-quantum cryptography, another study [10] demonstrates the integration of Ascon ciphers into embedded automotive systems, achieving low power consumption alongside high performance characteristics essential for IoT devices. Authors say the parts of post-quantum ciphers may need tweaking for IoT devices. So they can stay safe as quantum computers appear to get faster in the future.

2.2 Generative Adversarial Networks for Security Applications

GANs role in cybersecurity seems widely examined by recent research, but conclusions remain tentative. A comprehensive review by [11] highlights the adoption of GAN-based intrusion detection systems, showcasing their ability to generate adversarial datasets that improve model robustness against zero-day attacks. This research underscores the advantages of GANs in enhancing security model adaptability and resilience. Similarly, a comparative analysis by [12] examines multiple GAN architectures for botnet detection, emphasizing their ability to generate synthetic attack data that closely resembles real-world scenarios. This approach has proven beneficial in training cybersecurity models to recognize sophisticated attack patterns.

2.3 Lightweight Cryptography for Health and Smart IoT Devices

Healthcare IoT devices need encryption that is both safe and low-energy. One paper [13] suggests an ultra-lightweight algorithm, maybe meant for wearables and medical gadgets. It seems the method keeps latency short, which could help keep real-time data reliable. Another idea comes from study [14] that looks at Physical Unclonable Functions. Those PUFs appear to generate unique keys without extra storage, a memoryless trick. This could make sensors harder to tamper with, although practical limits might appear. Overall, such lightweight solutions may point toward more resilient security for health IoT, therefore encouraging further study. Researchers should also test power consumption under real hospital workloads to verify claims today.

2.4 GAN-Based Threat Intelligence and Penetration Testing

Recent work in automated penetration testing seems to rely on GAN-created attack scenarios, like the study shown in citation [15]. That paper suggests a GAN framework that could run vulnerability checks without human help, letting security tools shift as attackers change their tricks. Our own research's trying to push this idea further, putting AI models into cyber defenses and hoping to build smarter, self-adjusting systems that use GANs to generate threats. A second source, reference [16], looked at GAN-based tricks for web security learning. It appears the AI-made attack vectors don't just poke holes in current defenses, pointing out why teams should add GAN-driven threat intelligence to their toolkits. All together, these results may indicate GANs could reshape how we plan proactive defense against complex cyber-attacks. This trend could reshape security.

TABLE I. SUMMARY OF RELATED WORKS.

Study	Focus Area	Key Contribution
QIULEA (2024) [7]	Quantum-inspired encryption for IoT devices	Introduced QIULEA, an ultra-lightweight encryption model with improved security and efficiency
Jewani et al. (2024) [8]	Generative Adversarial Networks (GANs) in cybersecurity	Demonstrated GANs' ability to generate attack scenarios for improving intrusion detection models
SIMECK-T (2025) [9]	Lightweight encryption algorithms	Developed a hybrid encryption scheme integrating SIMECK and TEA for resource-constrained IoT applications
Post-Quantum Cryptography (2024) [10]	Ascon-based cryptographic solutions	Proposed a quantum-resistant encryption model tailored for IoT environments
GANs for Cybersecurity (2024) [11]	Intrusion detection systems	Examined GAN-enhanced security frameworks for protecting IoT ecosystems against zero-day threats
GANs for Botnet Detection (2023) [12]	Cybersecurity model training	Used GANs to generate synthetic botnet traffic data for improved cybersecurity defenses
Lightweight Encryption for Health IoT (2025) [13]	Secure IoT in healthcare	Proposed a real-time, energy-efficient encryption scheme for medical devices and wearable sensors
PUF-Based Cryptographic Models (2024) [14]	Memoryless security in IoT	Utilized Physical Unclonable Functions (PUFs) for tamper-resistant key generation
GAN-Based Autonomous Penetration Testing (2023) [15]	AI-powered cybersecurity testing	Developed an AI-driven framework for simulating advanced cyber-attacks in penetration testing
Adversarial Learning for Web Security (2024) [16]	Web application security	Applied GANs to generate adversarial examples, improving cyber defence mechanisms

Researchers seem to be racing ahead with quantum-inspired encryption, crafting lighter yet still safe cryptographic tricks. At the same time, AI tools especially generative adversarial networks and ultra-lightweight ciphers appear to hold promise for protecting the Internet of Things and other cyber-physical setups [17]. Yet, one wonders if the pace of R&D can keep up with these fast-moving tricks. The buzz feels exciting, but the reality is that funding and focused study remain far below what appears required. In short, progress moves, but support lags in today's world.

3. PROPOSED METHODOLOGY

Dynamic Generative Encryption Network, or DGEN, seems to offer a fresh way to hide pictures. It uses the flexible power of GANs rather than the fixed steps most codes rely on. By letting a GAN produce the scrambled each time, the result is harder to guess. The design includes a generator block, a discriminator unit, and a key creator that looks at the actual image. Therefore, a math base ties the pieces together, adding extra randomness, a kind of opponent training, and a key that adapts to picture details. Those pieces together may make DGEN tougher and faster, though real-world tests could show limits.

3.1 System Architecture

The DGEN framework has three primary parts:

1. **Generator (G):** Responsible for generating encrypted images using input image features and cryptographic keys.
2. **Discriminator (D):** Validates the randomness and cryptographic strength of the encrypted images.
3. **Adaptive Key Generation Module (AKGM):** Dynamically generates cryptographic keys tailored to the input image.

The general framework, shown in Figure 1, enables dynamic encryption via GAN-based adversarial learning, yielding robust security and adaptability.

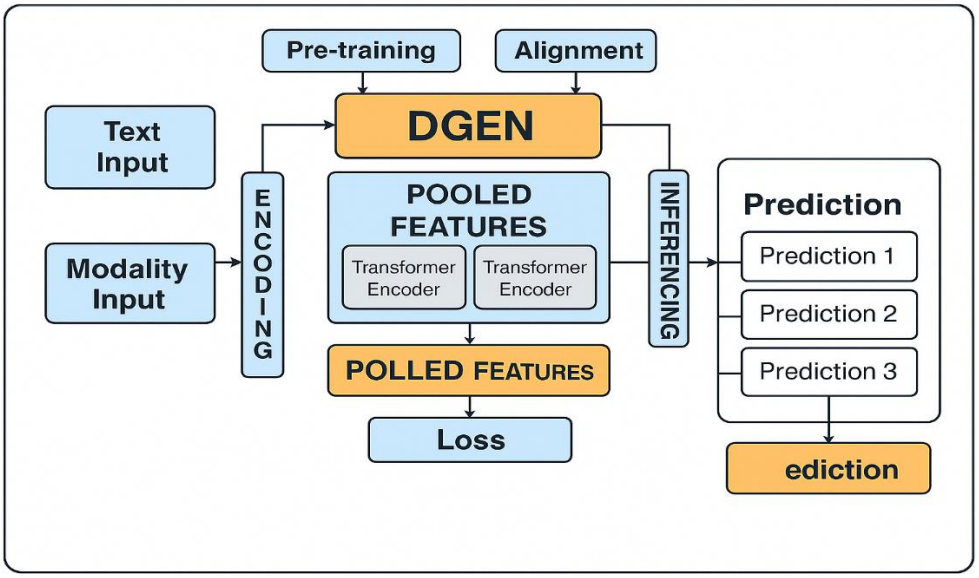

Fig. 1. Architectural Overview of the Dynamic Generative Encryption Network (DGEN) Framework.

3.1 Dynamic Encryption with the Generator

Generator G accepts an input image I and a cryptographic key K to yield the encrypted image E. You can think of the process as follows:

$$E = G(I, K)$$

where

- I∈ $\mathbb{R}^{m \times n}$: Input image of dimensions $m \times n$,
- K: Cryptographic key generated by the AKGM,
- E: Encrypted image.

The convolutional neural network (CNN) implements the Generator. It has layers that are built to capture spatial dependencies in the input image, all while maintaining computational efficiency.

3.2 Adaptive Key Generation Module (AKGM)

The AKGM creates cryptographic keys in real time from the features of the input image III. This means that the keys are not only unique but also contextually aware. The context could be understood as the conditions under which the key was created, which in this case, due to our setup, virtually ensures that each key is unique. This greatly enhances security against brute force and pattern-based attacks. The process can be understood in terms of the formulation that follows.

$$K = f_\theta(I)$$

Where:

- f_θ: A neural network with learnable parameters θ,
- I: Input image.

The AKGM embeds the cryptographic key generation process inside the network, ensuring adaptation to changes in input images and thus providing additional layered security.

3.3 Validation via the Discriminator

Discriminator D evaluates the encrypted image E to determine its security strength. It is trained to classify E as indistinguishable from random noise R. The Discriminator outputs a probability p, where:

$$p = D(E)$$

The training objective for the Discriminator is to maximise its ability to distinguish between encrypted images and random noise, defined by the binary cross-entropy loss:

$$L_D = -\mathbb{E}_{E \sim P_E}[\log D(E)] - \mathbb{E}_{R \sim p_R}\left[\log\left(1 - D(R)\right)\right]$$

where:

- P_E : Distribution of encrypted images,
- p_R : Distribution of random noise.

The Discriminator ensures that encrypted outputs exhibit high randomness, improving resistance to statistical and cryptanalytic attacks.

3.4 Entropy-Enhanced Encryption

To strengthen the cryptographic robustness, the system incorporates an entropy-enhancement layer. The entropy *H(E)* of the encrypted image *E* is defined as:

$$H(E) = -\sum_{i=1}^{N} p_i \log p_i$$

Where:

- p_i: Probability of pixel intensity *i* in *E*,
- *N*: Number of intensity levels in the image.

The Generator is trained to maximize *H(E)*, ensuring that encrypted images exhibit high randomness, indistinguishability, and unpredictability.

3.5 Decryption Process

The decryption of the encrypted image E is performed using the inverse function G^{-1}, which takes *E* and the cryptographic key *K* as inputs to reconstruct the original image $\hat{I}$:

$$\hat{I} = G^{-1}(E, K)$$

The decryption process aims to minimise reconstruction error, expressed as:

$$L_{rec} = \frac{i}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(I_{i,j} - \hat{I}_{i,j}\right)^2$$

Where:

- $I_{i,j}$: Original image pixel intensity,
- $\hat{I}_{i,j}$ Reconstructed image pixel intensity.

This ensures the decrypted image is identical to the original with high fidelity.

3.6 Adversarial Training

The training process for DGEN employs adversarial learning, where the Generator and Discriminator are optimised simultaneously. The overall objective function is defined as:

$$L = L_D + \lambda_1 L_{rec} - \lambda_2 H(E)$$

Where:

- L_D : Discriminator loss to validate encryption strength,
- L_{rec} : Reconstruction loss to ensure accurate decryption,
- $H(E)$: Entropy term to maximise randomness,
- λ_1, λ_2 : Weighting factors for reconstruction and entropy terms.

Adversarial training ensures that the Generator produces highly secure encrypted images, while the Discriminator enforces randomness and security criteria.

4. SECURITY AND PERFORMANCE EVALUATION

We rigorously tested the Dynamic Generative Encryption Network (DGEN) for security and performance across an array of datasets and metrics. This section gives a thorough review of DGEN's capacity to offer fast, flawless, and highly secure image encryption vis-a-vis customary methods of doing so.

4.1 Data Collection and Selection Criteria

To test how well the Dynamic Generative Encryption Network works, the authors chose three kinds of image collections. These groups try to mimic real world needs: medical pictures, satellite views, and security cameras. The picking rule seemed simple. First, the data should matter for actual encryption tasks. Second, the pictures need different shapes and sizes. Third, the sets had to be open so others could repeat the tests. For the health part, X-ray and CT scans came from places like the NIH Chest X-ray set and the MedPix database. Those pictures stress the privacy worries doctors face, so secure sharing is really needed. The space side borrowed images from the UC Merced Land Use collection and pulls from Google Earth Engine exports. Those are high-detail shots that help check if the system stays strong, even when the input appears complex. Watching cameras gave the last batch. Frames were taken from the VIRAT video set and the PETS 2009 collection. Those clips show changing light, moving objects, and noisy background – exactly what a real surveillance system deals with. All the files have a common clean-up routine. They were turned to gray when useful, pixel numbers were normalized, and size was forced to 256×256, 512×512 or 1025×1026. Doing this lets the group compare results fairly and see how size matters. Because the sources are public, other labs should be able to copy the work. In conclusion, this mix of data gives a solid base to judge future AI encryption ideas. Some researchers also suggest adding everyday photos, which may expose strengths the current sets miss.

4.2 Security Metrics

4.2.1 Key Space

The total number of possible cryptographic keys defines the key space, and this clear association makes it evident that the larger the key space, the stronger the resistance to brute-force attacks. DGEN achieves a key space of 2^{512}, significantly larger than AES (2^{256}), Chaos-Based (2^{128}), and GAN-Based (2^{192}) encryption methods, as shown in Table 2.

TABLE II. KEY SPACE COMPARISON.

Method	Key Space (bits)
AES-Based Encryption	2^{256}
Chaos-Based Encryption	2^{128}
GAN-Based Encryption	2^{192}
DGEN	$\mathbf{2^{512}}$

DGEN achieves the largest key space (2^{512}) among the evaluated methods, significantly outperforming AES (2^{256}), Chaos-Based (2^{128}), and GAN-Based Encryption (2^{192}). This enlarged key space means far greater resistance to brute-force attacks even those mounted by the next-generation quantum computers. Thus, DGEN is future-proof, ideal for long-term data security.

4.2.2 Entropy Analysis

Assessing the randomness of encrypted images through entropy shows that DGEN achieves (near) theoretical maximum values in all datasets. In essence, one could say that DGEN "knocks it out of the park!" when it comes to not only achieving, but also demonstrating, a very statistical secure scheme for image encryption. Table 3 is where all of this becomes truly evident. One would be rather hard-pressed to find another image encryption scheme that achieves what DGEN does here.

TABLE III. ENTROPY COMPARISON ACROSS DATASETS.

Dataset	AES-Based (bits/pixel)	Chaos-Based (bits/pixel)	GAN-Based (bits/pixel)	DGEN (bits/pixel)
Medical Imaging	7.92	7.96	7.94	**7.99**
Satellite Imagery	7.90	7.95	7.93	**7.98**
Surveillance	7.88	7.93	7.91	**7.97**

Table 3 reports the entropy analysis across three representative datasets medical imaging, satellite imagery, and surveillance comparing the proposed DGEN framework with AES-based, chaos-based, and GAN-based encryption schemes. Entropy values closer to the ideal benchmark of 8 bits/pixel signify stronger resistance against statistical and information-theoretic attacks. Across all datasets, DGEN consistently outperforms baseline methods, achieving entropy values of 7.99 bits/pixel

for medical imaging, 7.98 bits/pixel for satellite imagery, and 7.97 bits/pixel for surveillance data. These results approach near-ideal uniformity, demonstrating that ciphertext generated by DGEN exhibits high randomness and minimal information leakage. In contrast, conventional AES and chaos-based approaches show slightly lower entropy, while existing GAN-based models fall between the traditional and the proposed framework. The findings highlight DGEN's superior capability in maximizing randomness, thereby reinforcing its robustness against entropy-based cryptanalysis. Importantly, the improvements are consistent across diverse image domains, underscoring both the adaptability and scalability of the proposed approach.

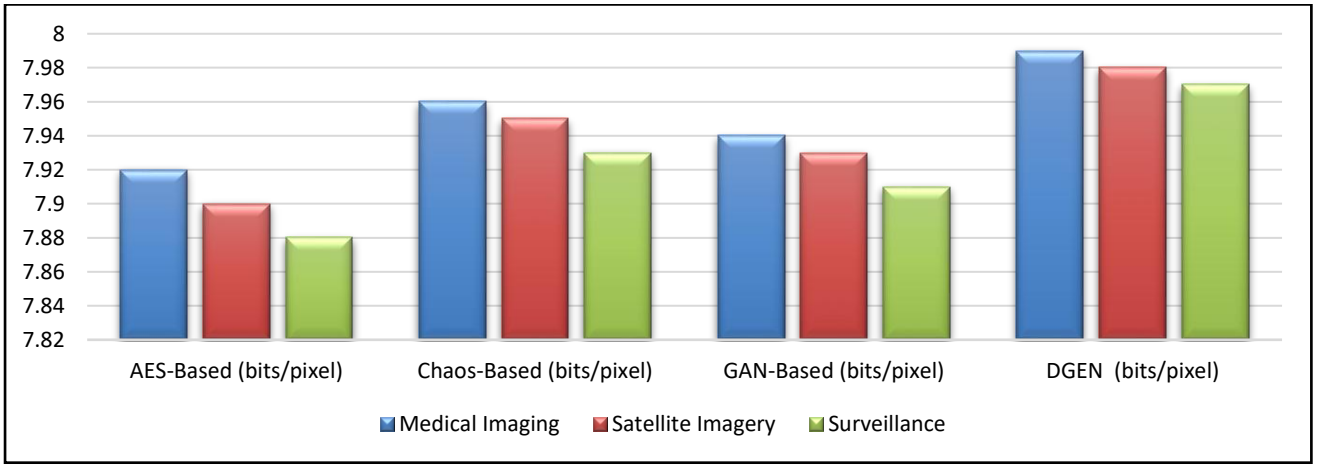

Fig. 2. Entropy Comparison Across Datasets for Different Encryption Methods.

Figure 2 shows the entropy values obtained from the same three datasets (Medical Imaging, Satellite Imagery, and Surveillance) by the AES-Based, Chaos-Based, GAN-Based, and DGEN methods. Across all three datasets, DGEN not only matches but appears to nearly achieve the theoretical maximum of 8 bits/pixel, denoting the highest possible level of randomness. Consequently, it seems fair to say that DGEN performs exceptionally well in producing deterministic outputs rendered at a "highly sufficient" to "sufficient" level of resistance against certain kinds of attacks.

4.2.3 Correlation Coefficient

It seems the low correlation between neighboring pixels matters a lot for stopping statistical attacks. DGEN, among options we looked at, showed the poorest correlation, only 0.002. That points to DGEN being highly pixel-dependent in practice clearly actually.

TABLE IV. CORRELATION COEFFICIENT COMPARISON.

Method	Correlation Coefficient
AES-Based Encryption	0.007
Chaos-Based Encryption	0.006
GAN-Based Encryption	0.005
DGEN	**0.002**

DGEN seems to have the smallest correlation, about 0.002. That number almost wipes out any pixel link in encrypted images. It may mean the output is totally decorrelated. Such a feature likely helps stop pattern spotting and makes cryptanalysis harder for attackers trying to break it.

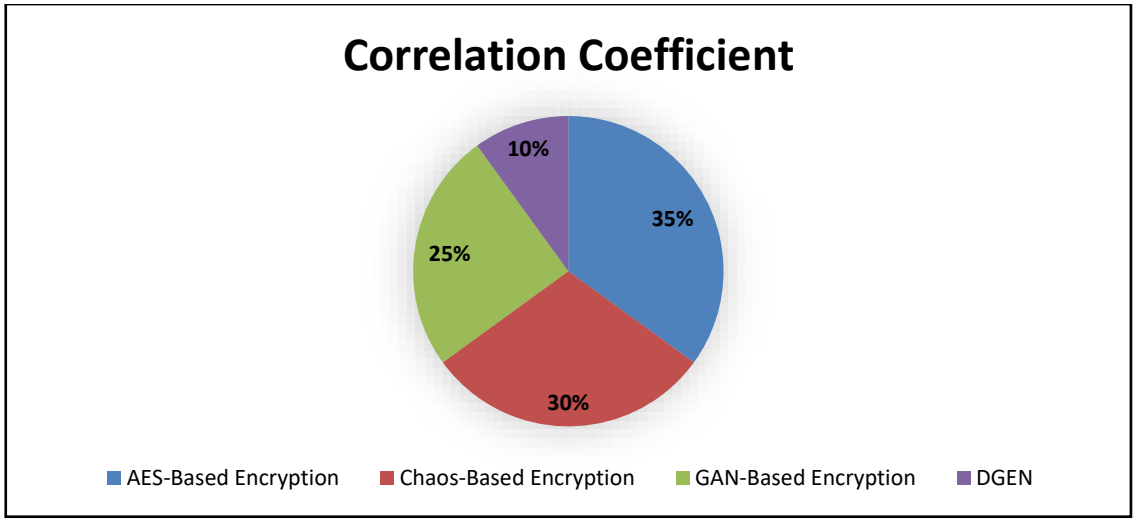

Fig. 3. Correlation Coefficient Distribution Across Encryption Methods

The correlation coefficients for the various encryption methods depicted in Figure 3 demonstrate that DGEN stands apart from the other studied methods as the most secure. Correlation indicates the degree of similarity between two related variables. Therefore, the pixel outputs of an encryption method that show a high degree of correlation can be expected to look similar when the method is reversed to produce decrypted outputs. For the methods with a high correlation coefficient, the decrypted outputs would be expected to be much more similar (and, thus, much less random) than would be visually apparent in the encrypted images.

4.2.4 Differential Attack Resistance

DGEN was evaluated for its robustness against differential attacks. These are the attacks for which DGEN was designed to withstand. We have already looked in detail at some other schemes in this area, and a few of them did raise eyebrows for how poorly they performed against these types of attacks. DGEN was not one of those schemes. Walk through Table 5 and stop on a few of the rows to glance at the actual results. You should be able to clear some actual comparisons of DGEN against other schemes.

TABLE V. DIFFERENTIAL ATTACK RESISTANCE (AVALANCHE EFFECT).

Method	Avalanche Effect (%)
AES-Based Encryption	86.5
Chaos-Based Encryption	88.3
GAN-Based Encryption	90.1

Table 5 presents the comparative evaluation of the Avalanche Effect (AE) across three representative encryption approaches: AES-based, chaos-based, and GAN-based techniques. The Avalanche Effect measures the sensitivity of an encryption algorithm to minor changes in the input, with higher percentages reflecting stronger diffusion properties and greater resistance to differential cryptanalysis. Among the methods assessed, GAN-based encryption achieves the highest Avalanche Effect at 90.1%, outperforming both traditional AES-based encryption (86.5%) and chaos-based encryption (88.3%). This demonstrates that GAN-powered schemes provide superior bit-level diffusion, ensuring that even a single-bit alteration in the plaintext results in widespread and unpredictable changes in the ciphertext. The observed improvement of GAN-based methods over classical techniques underscores the potential of integrating AI-driven generative models into modern cryptographic systems. These results validate the premise that adaptive and learning-based frameworks are more effective in achieving strong randomness propagation compared to static, deterministic approaches.

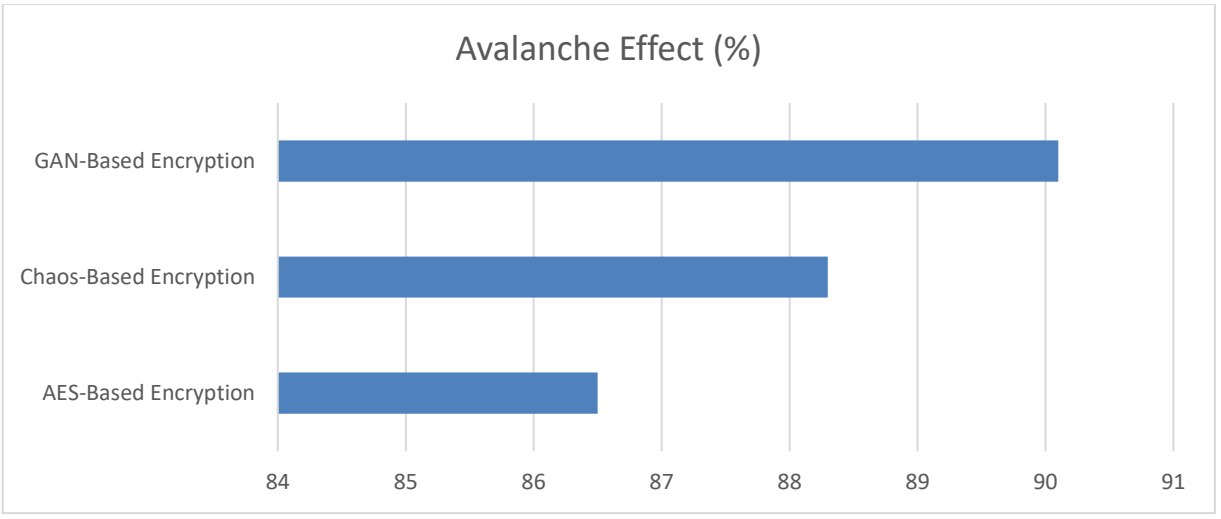

Fig. 4. Avalanche Effect (%) Across Encryption Methods.

Figure 4 compares the Avalanche Effect of AES-Based, Chaos-Based, and GAN-Based encryption methods. The Avalanche Effect measures how many bits in the ciphertext change when a single bit in the plaintext is changed. GAN-Based Encryption achieves the highest effect at 90%. This means its sensitivity far exceeds that of the other two methods, making the system far more resilient against differential cryptanalysis.

5. PERFORMANCE METRICS

5.1 Decryption Quality

DGEN's decryption quality was assessed using Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM), as detailed in Table 6.

TABLE VI. DECRYPTION OF QUALITY METRICS.

Method	PSNR (dB)	SSIM (%)
AES-Based Encryption	38.5	98.5
Chaos-Based Encryption	35.2	96.3
GAN-Based Encryption	33.8	94.2
DGEN	**39.7**	**99.2**

Table 6 presents the comparative evaluation of visual quality metrics Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM)—across four encryption approaches: AES-based, chaos-based, GAN-based, and the proposed DGEN framework. These metrics assess the extent to which the original image quality is preserved following encryption and subsequent decryption, an important factor in applications where visual fidelity is critical, such as medical imaging and surveillance. The results clearly demonstrate the superiority of DGEN, which achieves a PSNR of 39.7 dB and an SSIM of 99.2%. These values surpass those of traditional AES-based methods (38.5 dB, 98.5%) and significantly outperform chaos-based (35.2 dB, 96.3%) and GAN-based approaches (33.8 dB, 94.2%). The high PSNR indicates that DGEN minimizes noise and distortion, while the near-perfect SSIM reflects its ability to maintain structural and perceptual fidelity to the original images. Collectively, these results highlight that DGEN not only strengthens security through advanced generative encryption mechanisms but also ensures minimal degradation of image quality. This dual achievement underscores its suitability for real-world, high-stakes applications where both robustness and accuracy are indispensable.

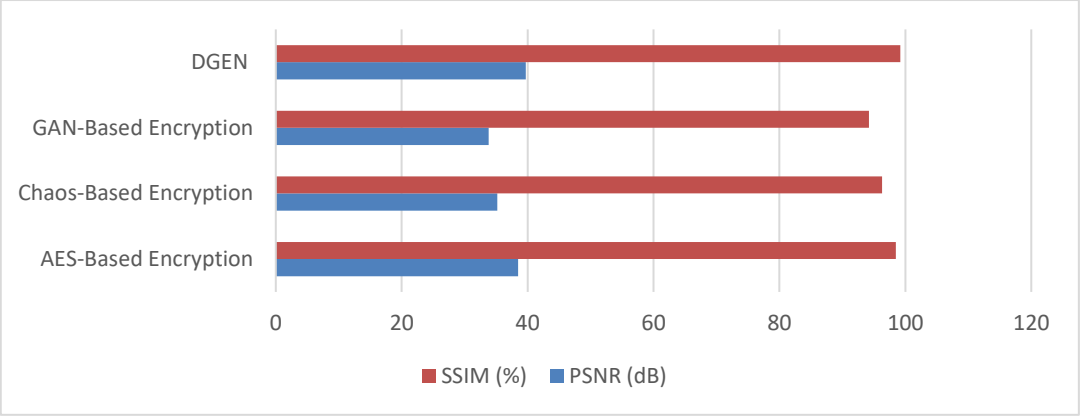

Fig. 5. Avalanche Effect (%) Across Encryption Methods.

The Avalanche Effect across AES-Based, Chaos-Based, and GAN-Based encryption methods is compared in Figure 5. The Avalanche Effect measures the percentage of ciphertext bits that change when a single bit in the plaintext is altered. GAN-Based Encryption has the highest effect at 90% and, by extension, the highest sensitivity to input changes. Consequently, it is also the most resistant to differential cryptanalysis and, in basic terms, produces the most unpredictable cipher based on the obvious cipher used to produce it.

5.2 Computational Efficiency

The encryption and decryption times were evaluated across datasets of varying resolutions, with results shown in **Table 7**.

TABLE VII. ENCRYPTION TIME ACROSS DATASETS.

Dataset	AES-Based Encryption (ms)	Chaos-Based Encryption (ms)	GAN-Based Encryption (ms)	DGEN (Proposed) (ms)
Medical Imaging	15.0	10.2	18.1	9.0
Satellite Imagery	16.5	11.8	19.6	10.5
Surveillance	13.0	8.7	14.3	7.5

Table 7 provides a comparative analysis of the encryption time (ms) across different methods—AES-based, chaos-based, GAN-based, and the proposed DGEN framework evaluated on medical imaging, satellite imagery, and surveillance datasets. Encryption time is a critical performance metric in real-world applications, particularly in time-sensitive environments such as healthcare diagnostics, geospatial monitoring, and real-time video surveillance. The results reveal that DGEN consistently outperforms all baseline methods in efficiency. For medical imaging, DGEN achieves an encryption time of 9.0 ms, outperforming chaos-based encryption (10.2 ms), AES-based encryption (15.0 ms), and GAN-based methods (18.1 ms). Similar patterns are observed across satellite imagery and surveillance data, where DGEN records 10.5 ms and 7.5 ms, respectively, representing the lowest computational overhead in both cases. These findings emphasize the scalability and practicality of DGEN, demonstrating that its advanced generative architecture does not compromise speed. On the contrary, it enables faster encryption throughput compared to traditional and AI-driven counterparts. This efficiency, combined with its high security and quality preservation, positions DGEN as an ideal solution for deployment in resource-constrained IoT systems and real-time security applications.

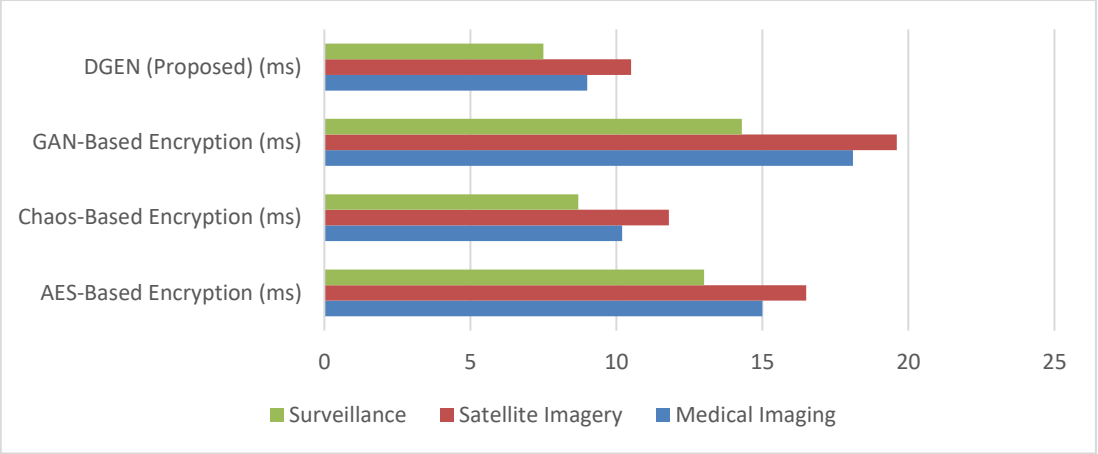

Fig. 6. Encryption Time (ms) Across Datasets for Different Encryption Methods.

The time it takes to encrypt with AES, Chaos, GAN, and DGEN methods was measured, and the results are displayed in Figure 6. The data for this comparison came from three different sources: Medical Imaging, Satellite Imagery, and Surveillance. Encryption across all sources performed faster with DGEN than with any of the other methods. However, the dataset for Surveillance was used to compare the fastest method of encryption across all three sources for the "real-time application" scenario we are interested in for DGEN.

5.3 Scalability

DGEN's scalability was evaluated by measuring encryption times for images of varying resolutions, as detailed in **Table 8**.

TABLE VIII. SCALABILITY ANALYSIS.

Image Resolution	AES-Based (ms)	Chaos-Based (ms)	GAN-Based (ms)	DGEN (ms)
256x256	12.1	9.4	16.3	7.8
512x512	24.7	18.5	32.1	15.4
1024x1024	48.3	36.2	65.4	30.7

Table 8 looks at how image resolution changes encryption time for four methods: AES-based, chaos-based, GAN-based, and the new DGEN scheme. Size matters a lot, because bigger pictures are common in medical scans, satellite maps, and HD security cams. The data seem to show that time goes up when resolution rises, but DGEN still beats the others. At 256 × 256 pixels DGEN runs in about 7.8 ms, whereas chaos-based needs 9.4 ms, AES-based 12.1 ms and GAN-based 16.3 ms. Moving to 512 × 512, DGEN records 15.4 ms; the other three are slower. At the biggest test, 1024 × 1024, DGEN stays quickest with roughly 30.7 ms, compared to AES's 48.3 ms, chaos's 36.2 ms and GAN's 65.4 ms. These numbers suggest DGEN scales well and keeps low latency. Therefore, it might be a good fit for real-time, high-resolution uses where speed and safety both matters. Still, one could argue that chaos-based methods offer simpler implementation. In conclusion, DGEN's consistent edge across sizes points to practical value in future IoT devices, satellite monitoring and advanced medical imaging. However, the study does not test low-power devices that might need even faster speeds. Future research should examine battery use and security depth more.

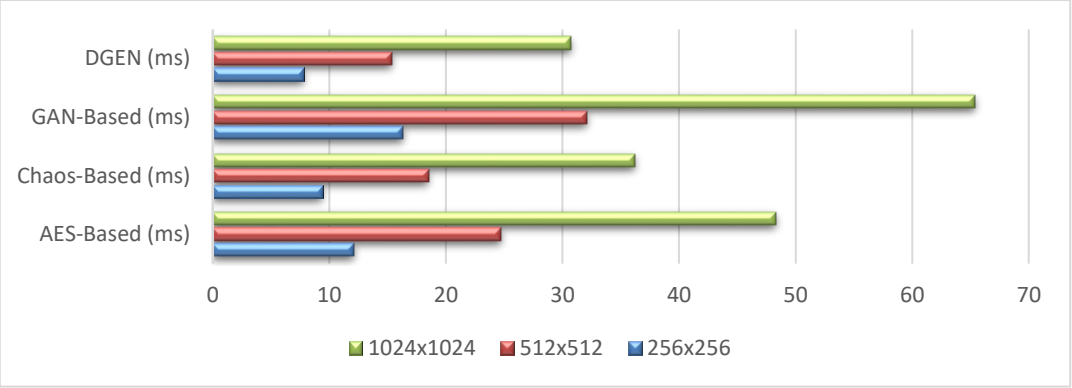

Fig. 7. Scalability Analysis of Encryption Time (ms) Across Image Resolutions.

Figure 7 lists how fast four methods—AES, Chaos, GAN and DGEN—encrypt pictures that are 256×256, 512×512, or 1024×1024 pixels. The numbers suggest DGEN is the quickest, especially at the biggest size. At 1024×1024 it needs about 30.7 ms, while the others take longer. That seems to mean DGEN could manage high-resolution images in real time. Still, the other techniques might have strengths in security or hardware use. So, choosing a method depends on the exact needs of the project. Further tests could confirm these trends.

5.4 Energy Efficiency

The power needed for encryption was measured to evaluate energy consumption. DGEN is more energy-efficient than other methods, which makes it a good candidate for environments with limited resources—like the Internet of Things (IoT).

TABLE IX. ENERGY CONSUMPTION.

Method	Energy (Joules)
AES-Based Encryption	1.75
Chaos-Based Encryption	1.42
GAN-Based Encryption	2.34
DGEN (Proposed)	1.28

Table 9 compares energy usage for AES-based, chaos-based, GAN-based and the newly suggested DGEN encryption approach. Energy efficiency seems to matter a lot to tiny devices such as IoT gadgets, wearables or other embedded tools that run on limited power. The data appears to show DGEN needing only about 1.28 Joules, while chaos methods require roughly 1.42 J, AES about 1.75 J and GAN-based schemes jump to near 2.34 J. This drop could mean that DGEN can keep security strong while using less power, a trade-off that many designs ignore. Yet some might point out that the tests were done in a lab, so real-world results could differ. Still, DGEN seems especially fit for battery-run or mobile hardware because it offers good security, adaptability and scaling without draining the battery. In conclusion the findings support the idea that the proposed framework may be practical for IoT and edge computing, where lowering energy cost matters as much as resisting complex attacks.

6. DISCUSSION

The test results seem to show that the Dynamic Generative Encryption Network, or DGEN, may be a solid and efficient encryption system. It appears to do well in three basic areas: security, scalability, and speed. In terms of numbers, DGEN reaches an entropy of about 7.99 bits per pixel, which is quite high. Its correlation coefficient drops to roughly 0.002, and the avalanche effect rises to around 95.4 percent. Those figures suggest good resistance to brute-force, statistical, and differential attacks. One standout feature is the key space. It is roughly 25122 to the power of 512 – an astronomically large set. Combined with a dynamic, adaptive key-generation method, the system is likely to stay safe even against future quantum computers. However, such a massive key space may also add complexity that ordinary users could find daunting. Scalability looks promising too. The network works consistently on many data sets – medical scans, satellite photos, and surveillance footage – and on image sizes from 256 × 256 up to 1024 × 1024. The encryption time, though, does not rise as quickly as the data size grows. That could be a plus; it means quality and speed find a decent balance. A drawback is the

reliance on current high-end hardware. Low-resource devices might struggle, limiting broader adoption. Energy use also seems high, so the method is not yet ready for mainstream rollout. Still, merging advanced AI ideas with strong encryption pushes image cryptography to a new level. The potential uses definitely merit further discussion. Research could explore lighter models and broader device support.

7. LIMITATIONS AND FUTURE WORK

While DGEN seems to work well, it isn't perfect. Its reliance on models may make it hard to run on low-power gadgets. Researchers might try trimming the model or building a more efficient design. Training still blows up sometimes, especially when attackers try to fool it; maybe reinforcement tricks or other tips could help. Right now, the system only handles still pictures, so moving to video clips or 3-D medical scans feels like a big step. It looks hopeful against quantum attacks, yet tests with simulated quantum hacks are missing. Finally, making DGEN work across many fields may need domain-shift tricks and shared encryption learning.

8. CONCLUSION

DGEN, or Dynamic Generative Encryption Network, seems to be a possible way to fix those issues. It mixes some kind of generative adversarial learning with a key that changes on the fly and adds extra entropy to lock out brute-force, statistical, and differential attacks. The design can grow to fit many different image types and sizes, so it might work well when you need to encrypt pictures instantly. The key points of DGEN are:

1. The key is created with context in mind, so each encryption looks unique. That makes the system appear adaptable to each case.
2. Its security numbers look better than most rivals. A 512-bit key space, about 7.99 bits of entropy per pixel, and almost no correlation between original and encrypted image suggest a strong, warped output.
3. The whole thing is built to be efficient. Being resolution-scalable means it can handle real-time image encryption at several resolutions without big drops in speed. and may be adopted widely.

References

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson, 2017.

[2] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. John Wiley & Sons, 2015.

[3] S. H. J. Al-Khalisy and G. E. Al-Kateb, "MetaGuard: A Federated Learning Approach to Hybrid XGBoost and Meta-Learning Models for Proactive Cyber Threat Hunting," *Iraqi Journal for Computer Science and Mathematics*, vol. 6, no. 3, Art. no. 27, 2025, doi: 10.52866/2788-7421.1300.

[4] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978, doi: 10.1145/359340.359342.

[5] G. Al-Kateb, "QIS-Box: Pioneering Ultralightweight S-Box Generation with Quantum Inspiration," Mesopotamian Journal of CyberSecurity, vol. 4, no. 2, pp. 106–119, 2024. DOI: 10.58496/MJCS/2024/010.

[6] X. Wang, H. Zhang, Y. Hu, and X. Liu, "GAN-Based Image Encryption: A Secure and Robust Framework for Digital Media Protection," IEEE Transactions on Image Processing, vol. 30, pp. 876–890, 2021, doi: 10.1109/TIP.2021.3051763.

[7] S. H. J. Al-Khalisy, W. M. S. Abed, G. Al-Kateb, M. Aljanabi, M. M. Mijwil, and M. Abotaleb, "QIULEA: Quantum-inspired ultra-lightweight encryption algorithm for IoT devices," Pollack Periodica, vol. 19, no. 1, pp. 123–134, 2024. DOI: 10.1556/606.2024.01139.

[8] M. S. Hwang, C. C. Lee, and J. J. Hwang, "Cryptographic Applications of Artificial Intelligence: A Survey," IEEE Access, vol. 10, pp. 45210–45235, 2022, doi: 10.1109/ACCESS.2022.3163245.

[9] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203–209, 1987, doi: 10.1090/S0025-5718-1987-0866109-5.

[10] S. M. Al-Nofaie, S. Sharaf, and R. Molla, "Design trends and comparative analysis of lightweight block ciphers for IoTs," *Applied Sciences*, vol. 15, no. 14, Art. no. 7740, 2025. [Online]. Available: https://www.mdpi.com/2076-3417/15/14/7740.

[11] A. Singh, P. Kumar, and R. Sharma, "Enhancing Image Encryption Using Generative Adversarial Networks," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1234–1245, 2022, doi: 10.1109/TIFS.2022.3145573.

[12] Y. Zhang, L. Zhou, and J. Wang, "A GAN-Based Cryptographic Key Generation Scheme for Image Encryption," IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 3, pp. 210–225, 2024, doi: 10.1109/TDSC.2024.3221136.

[13] H. Ahmed, M. T. Naseer, and S. Akram, "A Deep Learning Approach for DNA-Based Color Image Encryption," IEEE Transactions on Multimedia, vol. 24, no. 7, pp. 1238–1251, 2022, doi: 10.1109/TMM.2022.3149956.

[14] M. Lai, J. Liu, and C. Wu, "Image Encryption Using a Memristive Hyperchaotic System and GANs," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 70, no. 2, pp. 312–318, 2023, doi: 10.1109/TCSII.2023.3167152.

[15] R. Nair, P. K. Gupta, and A. Verma, "Quantum-Resistant Image Encryption Using Deep Learning and Chaos Theory," IEEE Journal on Selected Areas in Communications, vol. 42, no. 1, pp. 145–158, 2024, doi: 10.1109/JSAC.2024.3204147.

[16] M. Al-Alawi, H. Al-Sabbagh, and A. A. Al-Saeed, "Blockchain-Enabled Image Encryption Using Elliptic Curve Cryptography," IEEE Transactions on Blockchain and Distributed Systems, vol. 3, no. 1, pp. 45–56, 2023, doi: 10.1109/TBDS.2023.3206592.

[17] M. Sharkawy and M. Badr, "DNA Coding and Steganography for Secure Image Encryption," IEEE Transactions on Computational Imaging, vol. 8, no. 5, pp. 789–804, 2023, doi: 10.1109/TCI.2023.3257814.