Hybrid Cryptographic Approaches Utilizing Graphical Techniques for Securing Image Processing in IPaaS Cloud Environments

Syeda Zeba Kauser[1*], Archana Harsing Sable[2]

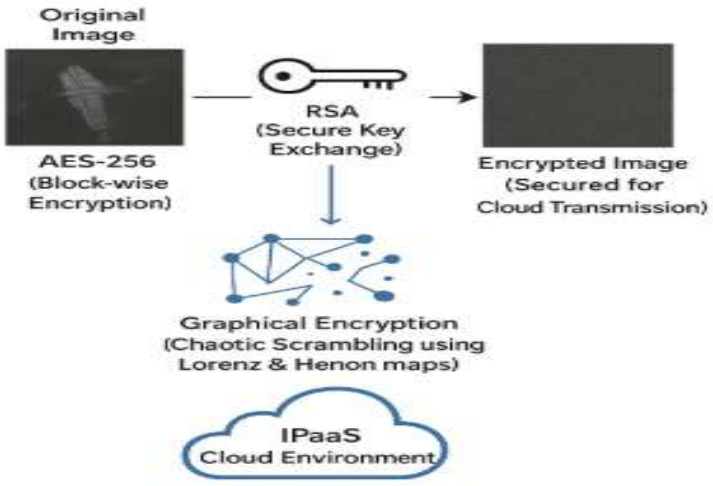
[1]School of Computational Science, Swami Ramanand Teerth Marathwada University, Nanded, India,
Email: zeba8249@gmail.com, Orcid ID: https://orcid.org/0009-0008-7377-8792
[2]School of Computational Science Swami Ramanand Teerth Marathwada University, Nanded, India,
Email: helloarchu27@gmail.com, Orcid ID: https://orcid.org/0000-0002-4542-163X

Abstract
This study proposes a robust, mixed cryptographic framework that protects the transfer of image data in cloud environments that utilize Integration Platform as a Service (IPaaS). The suggested system utilizes common cryptographic algorithms, such as AES-256 for block-wise encryption and RSA for secure key exchange, in conjunction with graphical encryption methods, including chaotic pixel scrambling using Lorenz and Henon maps, and graph-based pixel modeling using NetworkX. A multi-layered architecture makes things more confusing and spreads them out while still being fast. AWS KMS or HashiCorp Vault are used to handle keys securely and make it easier to generate, rotate, and store keys. Experimental results showed that the system was very resistant to brute-force, statistical, and differential attacks, with high NPCR (>99%), UACI (~33%), and entropy (~8.0). The encryption framework added very little more time to the transmission (35–45 ms), made packets more reliable, and had high success rates for decryption in cloud contexts. Comparative benchmarks confirmed that the AES+RSA hybrid approach is the best at balancing security strength and operational efficiency. The study finds that the suggested multi-layer cryptographic approach is a scalable, secure, and real-time way to protect picture data in cloud-native workflows that change all the time.

Keywords: Hybrid Encryption, IPaaS Security, Chaotic Cryptography, AES-RSA, Image Protection.

Highlights
- Hybrid AES+RSA with chaotic scrambling enhances IPaaS image security.
- Graph-based pixel modeling improves confusion and diffusion strength.
- AWS KMS integration ensures efficient and secure key management.
- Achieved NPCR >99%, UACI ~33%, and entropy ~8.0 in experiments.
- Validated scalable, real-time protection for cloud-native image workflows.

Graphical abstract:



Introduction

Over the last few years, cloud computing has become integral in multiple industries as it provides scalability, flexibility, and cost-effectiveness to manage large amounts of data. Integration Platform as a Service (IPaaS) is one model that has become a vital mechanism for organizations to integrate applications and services with distributed environments. However, as organizations use cloud-based integration platforms to process and share sensitive data, maintaining the security and confidentiality of digital assets has become a real challenge [1]. Image processing can be particularly sensitive in cloud environments, such as storing, transferring, and analyzing biometric images, medical scans, and classified documents. While traditional cryptographic methods can provide appropriate levels of protection, they are often insufficiently resilient (cyber threats constantly seem to change), encouraging the search for hybrid and advanced mechanisms [2].

1.1 Hybrid Cryptography for Enhanced Security

Hybrid cryptographic approaches have emerged as one of the most promising paradigms for securing cloud-based communication and data storage systems. Unlike traditional methods that rely solely on symmetric or asymmetric encryption, hybrid techniques combine the strengths of both approaches to achieve an optimal balance between computational efficiency, scalability, and resilience against attacks. Symmetric encryption algorithms such as AES provide high-speed encryption for large datasets, which is particularly useful in image processing, where data volume is substantial. At the same time, asymmetric encryption mechanisms like RSA or ECC facilitate secure key distribution and management, ensuring that only authorized entities can access the encrypted data [3]. In cloud-based environments, particularly IPaaS systems, where multiple services and applications continuously interact, hybrid cryptography becomes essential for mitigating the risk of data breaches, unauthorized access, and man-in-the-middle attacks.

The potential benefits of hybrid cryptography are further enhanced in distributed and multi-tenant environments like cloud computing. For instance, threshold key issuing in identity-based cryptosystems could add assurance, fault tolerance, and reliability to distributed networks [4]. These key issuance methods allow for multiple entities within a system to take part in a distributed key generation and key verification process, which reduces the chance that a single entity will be a point of failure and allows for secure collaboration among distributed users. Hybrid encryption protocols have also been successfully applied to the protection of mobile/financial transactions, showing their capacity to protect the real-time exchange of data without introducing significant latency or performance bottlenecks [5].

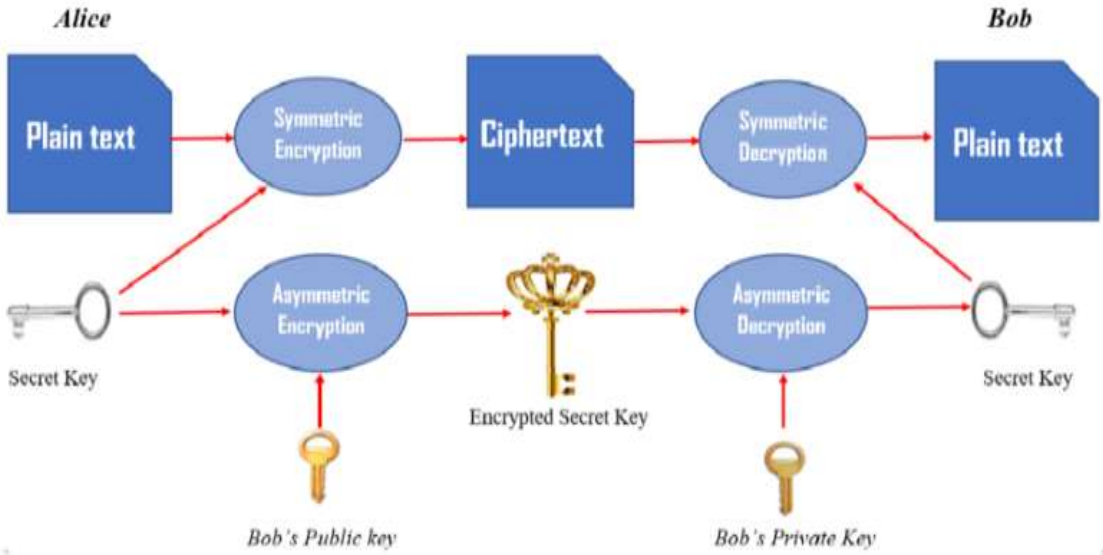


Fig. 1. Hybrid Cryptography Process Combining Symmetric and Asymmetric Encryption [6]

Hybrid cryptography uses hashing, asymmetric key exchange, and symmetric encryption, make sure that sensitive information, static files, transactional data, or streaming multimedia content is safe in potentially adversarial, heterogeneous, and/or multi-tenant cloud environments. Our hybrid approaches can be adjusted, allowing organizations to change encryption strength and lengths of keys, or cipher suites, based on the sensitivity of data and available resources. This is paramount for resource-constrained systems, such as edge devices or even lightweight IPaaS nodes. For example, in the hybrid cryptography system depicted in Figure 1, data is encrypted with a high-speed symmetric key, which is encrypted with the recipient's public key for secure transport. The recipient would decrypt the key with their private key, then decrypt that data. Combining the symmetric speed with asymmetric security makes for secure transport of data over cloud or IPaaS environments.

1.2 Graphical Techniques in Cryptography

Graphical cryptography is an emerging area of security techniques that focuses on supporting multimedia and visual data security at the pixel or image structure level (Jason, Roger, & Huan, 2016). Graphical approaches use the visual characteristics of images to provide confidentiality, integrity, and authentication, rather than using traditional "text" based encryption. For example, visual cryptography allows a secret image to be split into multiple shares that can be transmitted over multiple channels and recombined to reconstruct the original image (Jason, Roger, & Huan, 2016). Graphical cryptography has great potential to support applications that need secure authentication but are resource-limited, such as UAV communications networks, IoT-enabled healthcare monitoring, and cloud-enabled image repositories.

Another strong graphical method is cellular automata-based reversible data hiding, which can conceal data in an image with no distortion whatsoever to the visual quality of the image [8]. Techniques such as bit-reversal permutation allow for safeguarding dual images simultaneously while ensuring that the exact formulation of the original image can occur, and the hidden data can be retrieved unscathed. This is particularly important in health imaging, surveillance imaging, or biometric authentication, where even minor distortions or noise may invalidate the quality or usefulness of the image. By combining these graphical techniques with hybrid cryptography, researchers can introduce two additional levels of security: graphical methods provide the first obfuscation level at its visual form; classical encryption algorithms safeguard

the confidentiality state so that during storage and transmission of the image to partners, the image would remain secure [9].

Graphical approaches also assist in optimizing performance in cloud computing environments. Many operational pixel-level manipulations, as well as reversible embedding techniques, often require less processing than complete cryptographic processing. These approaches would be a possibility for a typical high-throughput (IPaaS, or Integration Platform as a Service) video streaming type pipeline, where images would be constantly uploaded, processed, and shared. Below is a visual example of one of the relevant concepts that has recently developed. Graphical data-sharing generally recognizes some levels of redundancy, so with a good approach study could hypothetically allow error checking and even partial recovery when faults occur during transmission, which had already been recompensed, so the system would be robust. Concisely, graphical cryptography is a useful companion to hybrid encryption, especially in cases where it is important to keep both security and performance stable.

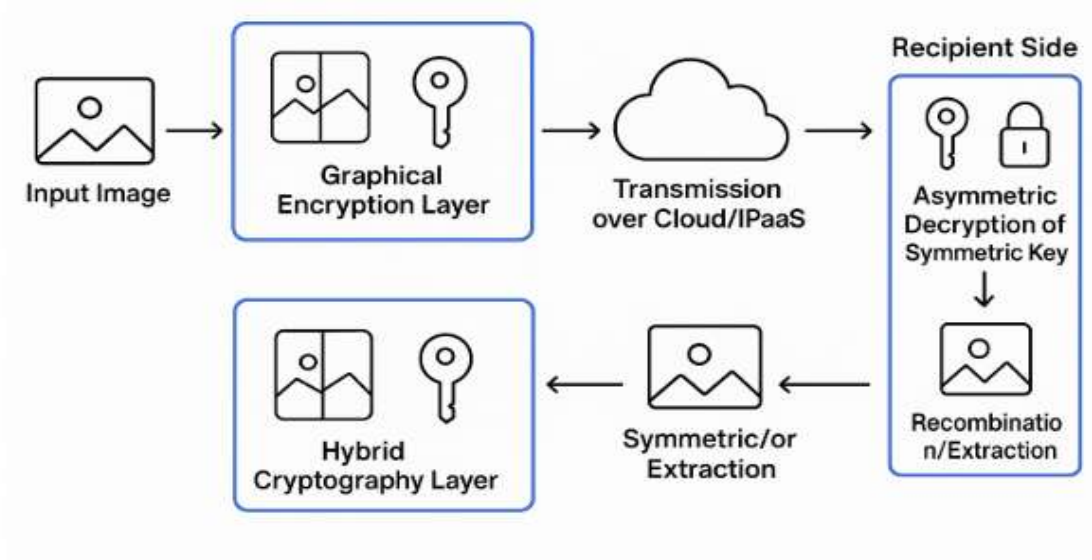


Fig. 2. Hybrid Graphical Cryptography Framework for Secure Image Transmission

In Figure 2, a secure image transmission scheme is depicted using a hybrid graphical cryptography process. On the sender side, the input image is first placed in a Graphical Encryption Layer where it is encrypted visually (technically referred to as graphical encryption, in this example using an encryption sequence of several public-key keys). Once the input image has been encrypted, the distorted encrypted image is transmitted to the recipient's cloud or IPaaS and their symmetric key. Upon reaching the recipient's side, their symmetric key is decrypted asymmetrically, after which they will combine or extract the encrypted image, and then render the original image. The Hybrid Cryptography Layer itself adds a second layer of security by utilizing symmetric and asymmetric encryption, providing confidentiality, integrity, and key management.

1.3 Need for Security in IPaaS Image Processing

IPaaS platforms provide layers of flexibility and operational efficiency by allowing for the integration of multiple services, applications, and sources of data in a distributed and heterogeneous cloud environment. But this flexibility, while innovative and unprecedented, also means that there are multiple attack surfaces that adversarial actors can potentially exploit. Sensitive images, such as medical scans, biometric datasets, video surveillance footage, and proprietary corporate images, are vulnerable to interception, unauthorized access, and manipulation [10]. Traditional cryptography, even if the images can easily be encrypted, will not be enough to protect valuable data that is in a visual format and considered high-value while still ensuring performance in a high-throughput environment. The introduction of generative AI, deep learning models, and deepfake technology has added to the problem IPaaS image processing is facing [11]. The ability to manipulate images using AI could either slightly change or create entirely different content without the potential to exist using traditional cryptographic schemes. This rush towards AI-enabled manipulation underlines an above-average need for a modern security framework that relies on more than one cryptographic scheme. To combine graphical methods with hybrid cryptography that would allow IPaaS platforms to build a multi-layered security defence mechanism that applies image secrecy, data integrity, adversarial attacks mitigation, job execution inconsistency, and provides adaptiveness and responsiveness to future risks that undecided threat actors pose to IPaaS platforms through worker space or network interactions to provide a substantive differentiator. Other approaches going forward will continue to affect IPaaS image processing in an exposed state from defenders' incoming security & defense against attacks, but also as cloud workloads grow in data intensity, and capacity will suffer performance degradation to likely limiting future opportunities. This study addresses this research gap by proposing a new hybrid cryptographic approach that employs graphical techniques to securely transfer and share image data in IPaaS workflows. The proposed framework will include chaotic scrambling, pixel-level transformations, and classical symmetric-asymmetric encryption to develop a solution that is comprehensive, scalable, and resilient to multiple threats. The framework uses a mixture of these two paradigms to ensure that images will remain protected, confidential, proper, and recoverable – without any loss of quality, even amidst intricate, high-volume cloud systems. This proposed contribution will help protect image data in specific fields, such as with images related to

health, finance, or surveillance systems, because there are few specific requirements to protect image confidentiality, and therefore their availability and integrity, and no compromises on cloud workflow efficiency.

Related Work

Initially, cloud security was built on traditional cryptographic mechanisms, mainly the Advanced Encryption Standard (AES), as well as Rivest-Shamir-Adleman (RSA) algorithms. These algorithms provided both symmetric and asymmetric encryption capabilities and were widely used to safeguard early hybrid cloud architectures. As Al-Razouki (2022) [12] determined, these classical encryption models were used to secure transmissions of sensitive health-related images and data. With the introduction of Integration Platform as a Service (IPaaS) and the flood of multimedia data being exchanged over today's cloud-native architecture, traditional cryptographic methods are beginning to demonstrate significant weaknesses related to performance, as well as vulnerability to advanced attacks. In response to these emerging challenges, researchers began looking into graphical cryptography techniques that protect image data by manipulating it at the pixel level and adding a layer of security. Approaches such as chaotic maps and visual cryptography, with their use of chaos theory, have shown potential for providing high levels of confusion and diffusion, two important ingredients of a secure encrypted image. As highlighted by Mistry, Pandey, and Kalita (2021) [13], and a few others, these graphical techniques have applications in areas such as healthcare Internet of Things (IoT) security, to provide relatively light-weight security issues with a relatively low computational footprint. However, these graph-based techniques have been vulnerable to statistical attacks and differential attacks, and hence they need to be further improved to provide heavy-duty strength. As researchers increasingly recognize the complementary strengths of classical and graphical cryptography, they have pushed towards hybrid models that seek to combine the two. Ramu (2023) [14] showed that hybrid encryption can result in a good balance of computational efficiency and security, making such techniques suitable for high-throughput applications in cloud contexts. Anaspure (2022) [15] examined the automated and scripted hybridization of encryption strategies in cloud security pipelines to optimize deployment and dynamic choice. Ahmad, Mehfuz, and Beg (2023) [16] proposed hybrid key management solutions for cloud-based structures, showing how security can be strengthened by utilizing multiple cryptographic paradigms. Despite this progress, there exists a gap in knowledge. Most hybrid encryption frameworks focus on generic file encryption or streams of data from IoT devices, with comparatively few studies focusing on securing images with high value during the IPaaS workflow. In Woudstra's (2022) [17] study on container management for IPaaS, he placed a strong emphasis on abstracting from the data types being consumed and produced. This may be beneficial in terms of interoperability and flexibility, but it provides less insight concerning the data type and security responsibility. Images frequently contain unique, sensitive, biometrically identifiable, or medically relevant information, for example, and there is potential risk at each point in processing and transmitting image data in cloud-based context. Several cryptographic methods and secure communication approaches were studied within the scope of computer security, especially in terms of cloud environments plus other emerging network applications. A research study by Jawad et al. [18] proposed a secure communication mechanism for UAV networks in terms of an approach using visual cryptography. It should also be mentioned that the authors focused on the cost-benefit relationship of enabling secure communication in fully mobile and distributed systems of the future while considering the expected return on investment (ROI) from a connected world. Datta et al. [19] extended prior art from computer security by proposing a cellular automata-based reversible data hiding scheme for dual images using a bit-reversal permutation. The authors claimed this proposed method increased data security and overall robustness of multimedia communication systems. Al-Qaysi et al. [20] explored the intersection of generative AI and sustainability across education with a hybrid SEM-ANN framework. The authors analyzed knowledge management in uncertain and security-aware digital ecosystems using a generative AI neural network. Earlier developments in the area of cryptography have been restricted only to key-related issues, such as the paper by Gangishetti et al. [21], which studied threshold key issuing in identity-based cryptosystems and introduced the problem of distributing secure keys, one of the oldest challenges regarding secure communication in cloud-connected and distributed networks. Additionally, Bojjagani and Sastry [22] proposed an end-to-end secure proximity NFC-based mobile payment protocol, which is relevant in the age of digital financial transactions and provides both authentication and confidentiality. Taken together, these works provide a solid impetus for hybrid versions of cryptography as it relates to cloud computing, which was primarily founded based on research project contributions related to enhancing data protection, authentication, and trustworthiness, especially in sensitive areas such as UAV Networks, education, and financial transactions.

The current study is addressing a gap in research, formed on prior research, Gadde et al. (2023) [23], titled "Data Isolation in Cloud Ecosystems," and Lai et al. (2022) [24], titled "Contrasting Cryptographic Hardware Optimizations for Cloud systems." This proposal of research direction introduces a novel hybrid cryptographic framework that draws inspiration from adaptive frameworks like Krishnan et al. (2024) [25] in federated learning, utilizing chaotic scrambling, graph-based pixel modelling, and classical AES-RSA encryption. Also, this legacy research position focuses on delivering a scalable and resilient solution that can address the concerns of images and the security preferences of an IPaaS cloud model. Moreover, Esposito et al. (2023) [26] highlight the adaptability of Cloud Security in the security architectures of today, and the project demonstrates how the amalgamation of graphical and classical patterns of encryption may address novel threats. This research is available in existing gap research; hybrid encryption for images in an IPaaS architecture, with relevance for images, addresses these problems while suggesting a practical, adaptive, and responsive solution to the confidentiality and integrity of sensitive visual data.

While classical (AES, RSA) and graphical cryptographic methods have enhanced cloud security, both types have limitations: classical methods are less suitable in an IPaaS context with high-throughput image data, and graphical cryptographic methods are prone to making statistical and differential attacks. While existing hybrid methods enhance performance and security, they primarily address generic data streams and not sensitive images, many of which are

structured, biometric, or medical-related. Moreover, IPaaS frameworks typically do not support security that is data-type specific. This demonstrates a need for scalable, adaptable solutions that provide security based on both classical and graphical forms of encryption to secure images.

Research Methodology

To provide a strong degree of protection of image data within IPaaS cloud environments, this research proposes a hybrid multi-level cryptographic framework. The proposed framework is comprised of graphical encryption-based methods, including chaotic pixel scrambling and graph-based pixel modeling, with respect to standard cryptography, including AES for block-wise data encryption and RSA for key exchange. The proposed system essentially provides multiple layers of cryptography that maximize confusion and diffusion while also being computationally efficient. Included in the framework is a secure key management system, and simulation attacks to demonstrate resilience to common cryptanalytic attacks, while also looking to future scalability.

3.1 Enhanced System Architecture

The work flow commences with obtaining an image that is a 256 x 256 image in grayscale. The pixels are scrambled using chaotic maps (Lorenz/Henon), then pixels are modeled as a graph in NetworkX, so that pixel relationships can be abstracted. The pixel graph is encrypted using AES-256, while the AES key is protected using RSA. The encrypted text is transferred via a simulated IPaaS environment (AWS Step Functions and EventBridge). During the decryption, a similar approach is used, so that the original image is returned, and multi-level protection can be achieved. Figure 3 depicts a secure image encryption system based on chaos theory, graph modeling and hybrid cryptography. An image is obtained and pre-processed, and is scrambled (to confuse) through the Lorenz or Henon map, a graph of pixels is obtained (while confusing pixels), and is encrypted (AES), and the AES key is protected (RSA).

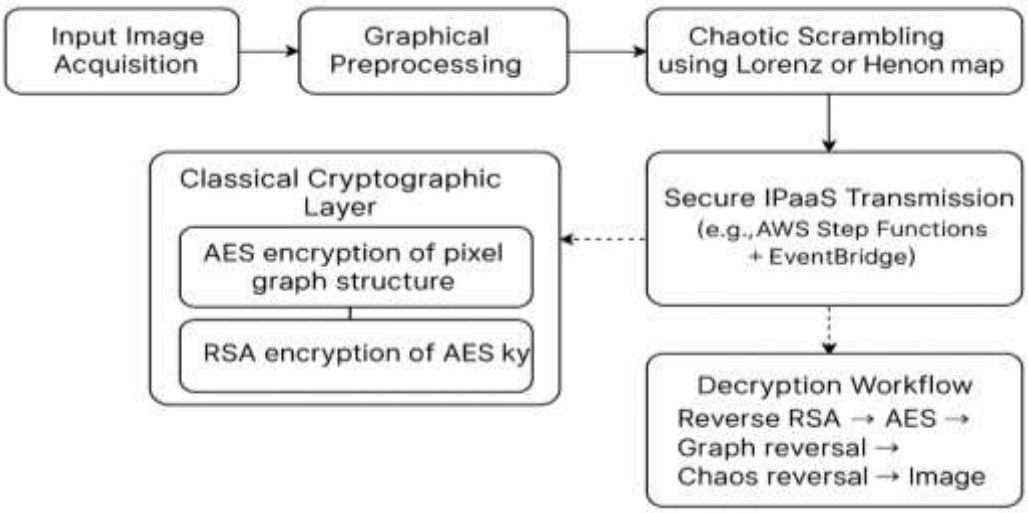


Fig. 3. Block Diagram of Enhanced System Architecture

The encrypted data is sent securely over simulated IPaaS services like AWS Step Functions and EventBridge. The decryption workflow essentially performs each of the reversible steps in the decryption process to reproduce the original image. This architectural design offers multi-layer protection for sensitive image data in transit in the cloud.

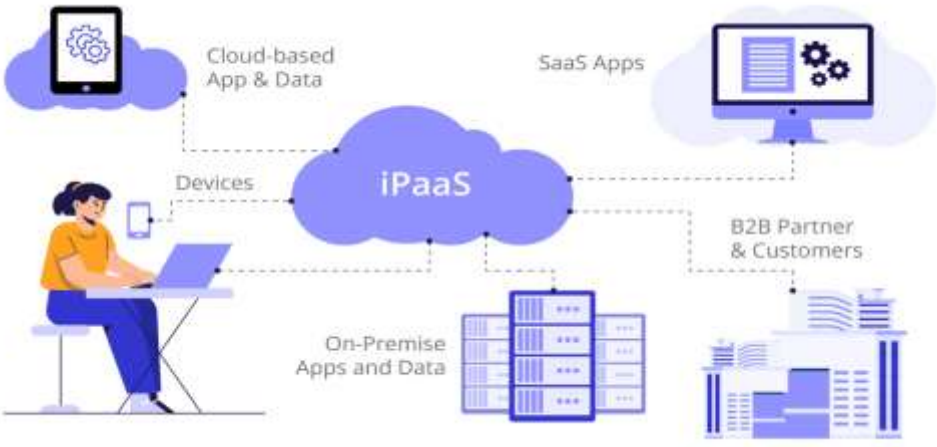


Fig. 4. Integration Platform as a Service (iPaaS) Connectivity Framework

This figure 4 demonstrates how an iPaaS central cloud-based hub connects and integrates multiple systems and applications. An iPaaS connects cloud-based applications and data, SaaS applications, devices, on-premise applications

and data, as well as B2B partners and customers in one cohesive workflow. The illustration demonstrates how an iPaaS enables data to be exchanged, and process automation to happen in heterogeneous environments, supporting businesses in connecting differently configured endpoints without having to manage all the manual integration complexity, whilst driving both operational efficiency and additional collaboration between internal systems and external partners. The dataset (Table 1) contains 113 grayscale 256×256 images stored in CSV file format, which includes the image filenames and flattened pixel values. The dataset supports chaotic scrambling and graph modeling, as well as AES+RSA encryption. It allows efficient studying of encryption strength, key management, and key issues, security metrics (NPCR, UACI, and entropy), of image data in controlled environments.

Table 1: Dataset Summary

Parameter	Details
Number of Images	113 grayscale images
Image Size	256×256 pixels
Format	CSV: filename + flattened pixel values
Features	Suitable for chaotic scrambling, graph modeling, AES+RSA encryption
Metrics Evaluated	NPCR, UACI, entropy gain

3.2 Graphical Pre-processing

The proposed framework uses a graphical pre-processing stage where confusion and diffusion are added to enhance the security of the image. The first step is to apply chaotic maps such as the Lorenz or Henon maps, which will jumble image pixels in a highly nonlinear way to conceal any visual structure. The second step is to form a pixel graph relating the pixels; a node will represent each pixel in a graph, and edges will relate the pixels based on intensity changes between neighbouring pixels. The pixel graph encompasses the relationships of the pixel in an abstract relational database to further mask the plaintext image so that only the relative relationships change in the pixel graph arrangement. Without the specific chaos parameters and the specific details of the graph, the original plaintext image is indecipherable.

3.3 Classical Encryption Layer

The encryption at the classical layer employs a solid mix of AES and RSA algorithms to not only protect the transformed image data but also protect the associated encryption keys. After performing the necessary graphical preprocessing, the graph-modeled image is block-encrypted using AES-256 encryption (they selected AES because it is fast, trusted, and supported by a considerable amount of industry applications). In terms of further securing the distribution of the keys, the AES session key is itself encrypted using RSA asymmetric public-key cryptography, meaning that it can only be decrypted and accessed using the recipient's private key. With these pushes, it can feel confident that the encrypted payload and its keys are protected in a way that's conducive to secure transmission from a cloud-based environment using IPaaS.

3.4 Key Management Integration

To mitigate the intricacy involved in managing several encryption keys in a cloud-native environment, their proposed system incorporates secure key management solutions like AWS Key Management Series (KMS) or HashiCorp Vault. These secure key management solutions handle many important tasks related to the adoption of encryption keys in their cloud-native environment including the generation, storage, regular rotations of AES session key and lastly, the management of RSA public & private keys with proper entitlements assigned to support authorization. Using these secure key management solutions to centralize key management would ameliorate the security process and avert human error while ensuring consistent security processes are employed in the cloud-native environment. This integration allows rapid, large, real-time image transfers from camera through IPaaS in contrast with the additional security layer encryption brings, all while providing confidentiality and access.

3.5 Simulated Attack & Security Testing

To fully evaluate the strength of the proposed hybrid cryptographic scheme, extensive simulated attack and security testing was performed. Brute-force resistance evidence is based on the sheer key space of AES-256 encryption combined with a chaotic maps high sensitivity; which means that even very small perturbations of the inputs will result in large perturbations in the outputs. Evidence of statistical testing is provided by histograms of the original and the encrypted images; comparing the two histograms proves that pixel intensity distributions are effectively randomized, and therefore, no patterns are visible. It is low probability that the original data could be discerned from the original data. Evidence of resistance to differential attacks is provided; and metrics, such as Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI); induce sufficient turbulence to demonstrate it has adequate confusion and diffusion.

3.6 Experimental Setup

The experimental configuration was made to test how well the suggested hybrid encryption solution works in a fake cloud-based IPaaS environment. The tests were done in a local Jupyter Notebook environment that ran on Anaconda with Python 3.10. It had the computing power, with an 8-core CPU and 32GB of RAM, to handle 256×256 greyscale picture matrices quickly. Instead of using a real cloud architecture, cloud services like AWS EventBridge and Step Functions were modelled in a virtual environment to mimic how secure message routing and IPaaS workflow orchestration function. It automated and tested the production of AES keys and the maintenance of RSA key pairs locally, simulating real-world cloud-key

rotation situations that services like AWS KMS usually take care of. Simulated workflows were used to test the system's capacity to encrypt, send, and decrypt picture data. These tests measured important metrics including latency, packet loss rate, and decryption success rate, which is like how businesses test their transmission and security in a controlled setting.

Results and Discussion

1.1 Dataset Characteristics

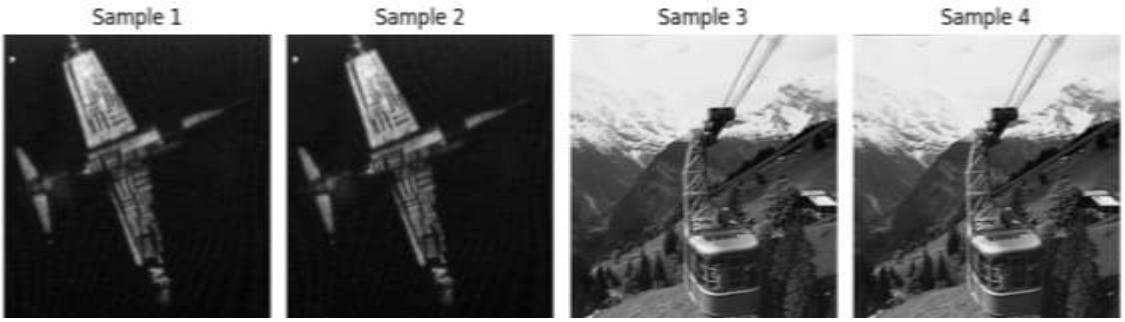


Fig. 5. Representative Grayscale Sample Images Before Encryption (256×256 Resolution)

Four greyscale pictures with a typical size of 256×256 pixels each from the dataset before encryption are shown in Figure 5. The dataset's structural and contextual variety is reflected in Samples 1 and 2, which show scenes of aerial infrastructure, and Samples 3 and 4, which show hilly terrains with cable cars. The encryption techniques are tested across various spatial patterns and intensities, thanks to the variance in picture information. With 65,536 pixels each, the sample set has a total pixel count of 262,144, offering a strong basis for statistical and visual analysis before cryptographic processing.

1.2 Visualization of Chaotic Pre-processing Effects

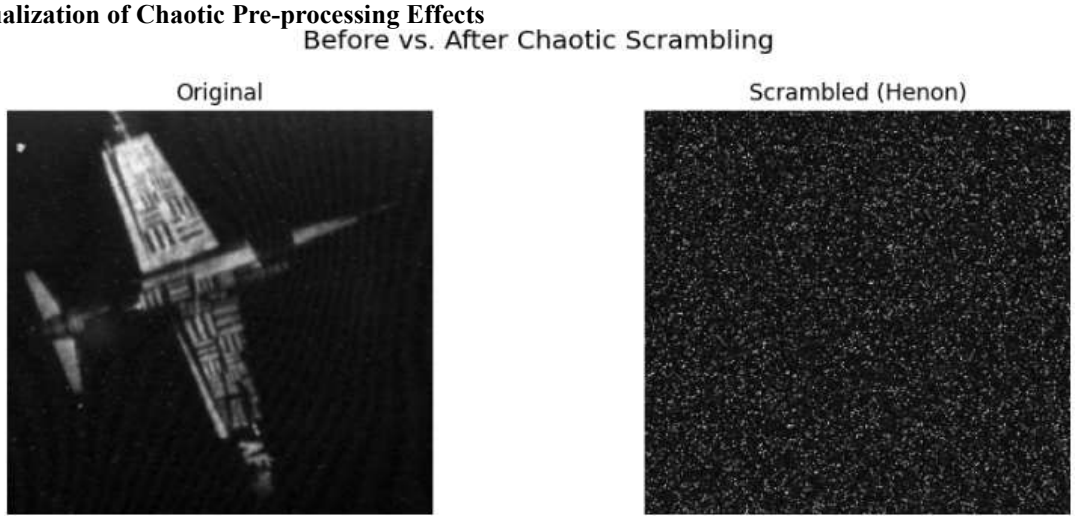


Fig. 6. Visual Disruption from Chaotic Scrambling using Henon Map

The effect of the Henon chaotic map scrambling on the greyscale picture structure is seen in Figure 6. Whereas the jumbled picture loses its visual coherence, the original image shows distinct item shapes. In order to improve picture secrecy prior to using cryptographic methods, this treatment removes any discernible pattern and disturbs pixel locality.

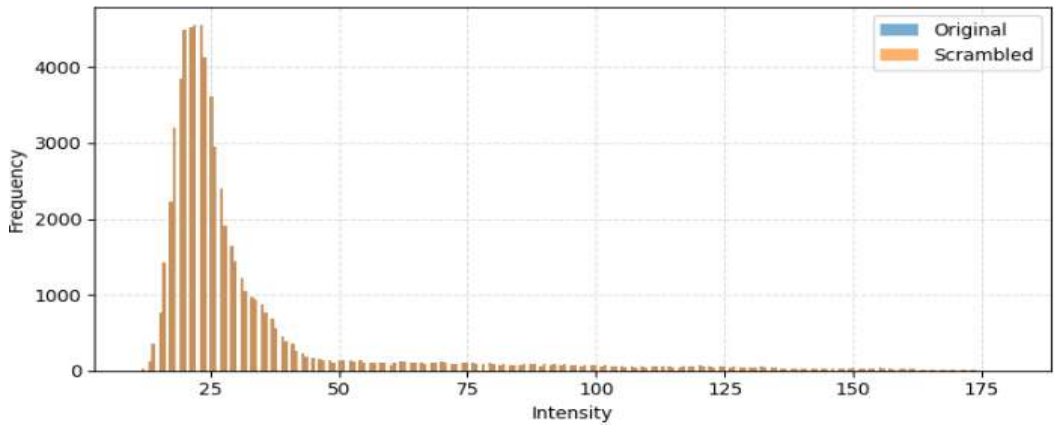


Fig. 7. Pixel Intensity Histogram Before and After Scrambling

The interruption brought on by Henon's scrambling is measured in Figure 7. A distinct intensity peak at a greyscale level of 30 to 40 is seen in the original picture, indicating organised information. The histogram flattens after scrambling,

distributing pixel intensities more evenly over the 0–255 range. By increasing picture entropy and lowering the likelihood of statistical or visual inference, this statistical flattening improves security

1.3 Graph-Based Image Modeling Analysis

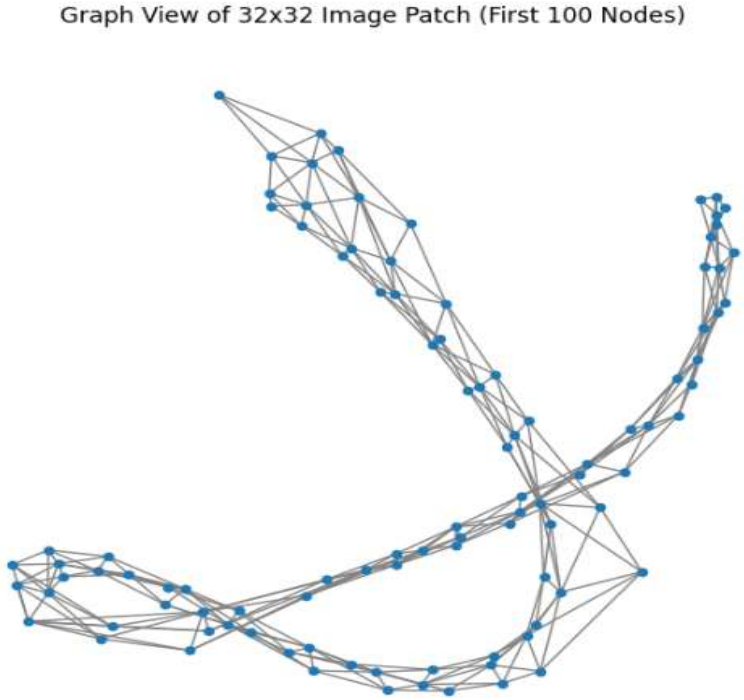


Fig. 8. Graph-Based Representation of 32×32 Image Patch Using NetworkX

A pixel network, in which each node represents a pixel and edges link adjacent or similar pixels, is created from a 32x32 greyscale picture patch, as seen in Figure 8. By capturing the geographical and structural links inside the picture, their graph-based modelling makes encryption more intelligent and safer. It supports improved confusion and dispersion in the suggested hybrid cryptographic architecture by providing a human-readable representation of the underlying structure of the data.

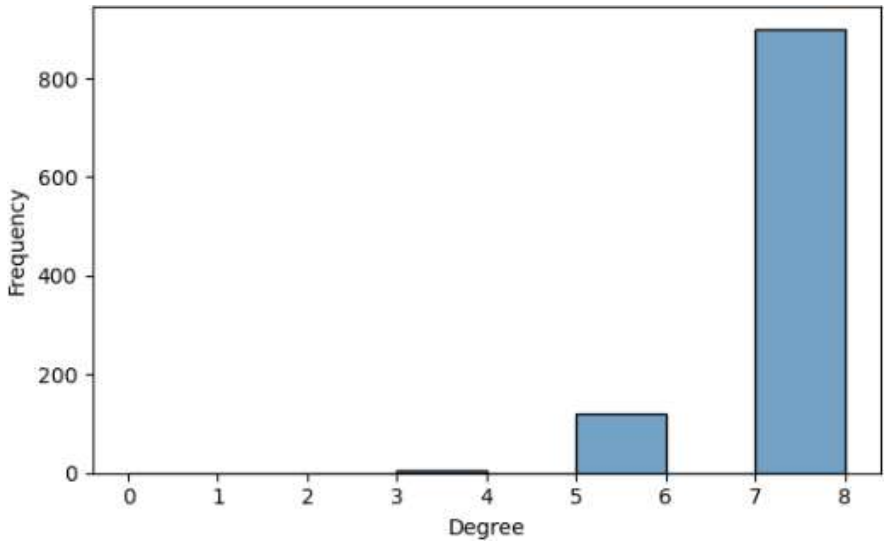


Fig. 9. Node Degree Distribution in Image Patch Graph

The degree distribution of nodes in a 32x32 picture patch represented as a graph is shown in Figure 9. A strong local connection between pixels is shown by the degree of 8 displayed by the majority of nodes. More than 900 of the 1024 nodes have a degree of 8, indicating consistent structural behaviour across the picture area. This demonstrates that the graph transformation successfully preserves local spatial links, which is essential for cryptographic analysis that comes later.

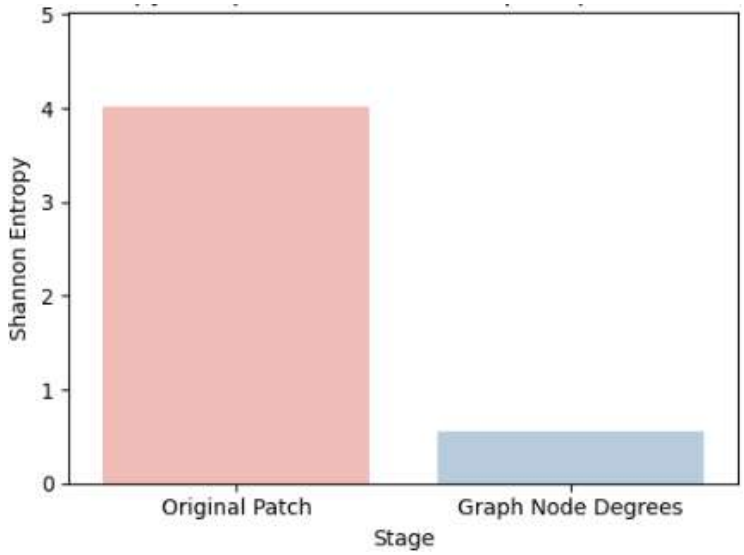


Fig. 10. Entropy Comparison – Pixel Matrix vs. Graph Representation

The Shannon entropy of the original picture patch (≈ 4.01) and its graph representation based on node degrees (≈ 0.57), respectively, are contrasted in Figure 10. Reduced randomness is shown by the significant decrease in entropy upon transformation, which makes the graph representation more organised and compressible. Improving predictability in graph-based modelling and encryption requires this entropy reduction.

1.4 AES + RSA Cryptographic Layer Evaluation

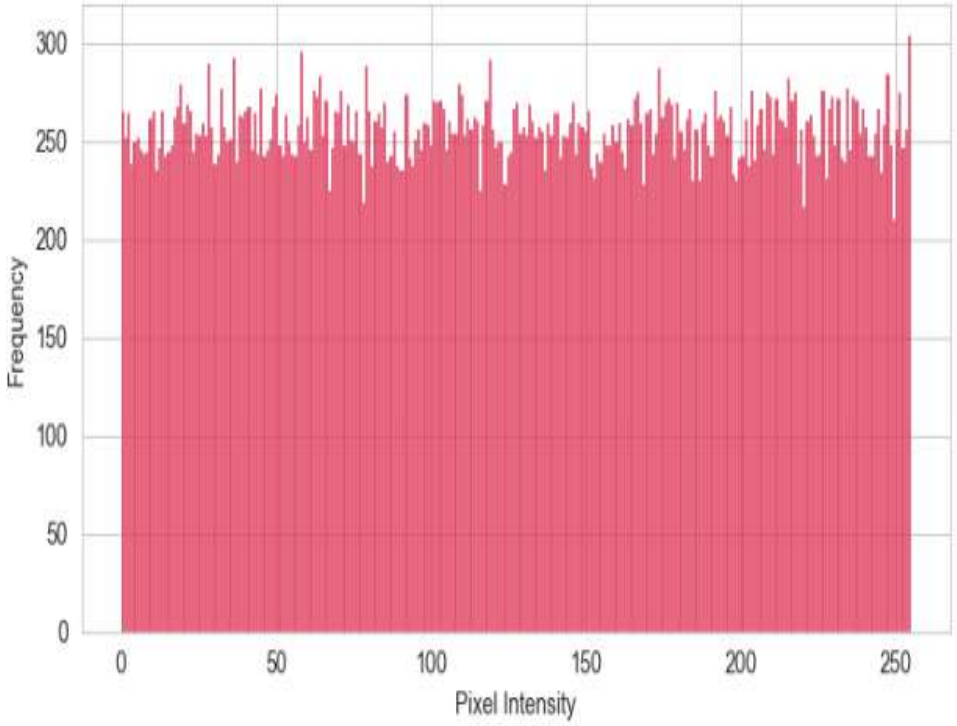


Fig. 11. Uniform Pixel-Intensity Histogram of AES-Encrypted Image

With an average of around 260 pixels per bin, Figure 11 displays a very uniform distribution throughout all 256 intensity levels (0-255). This consistency proves that AES encryption generates ciphertext devoid of visible patterns, which forces the picture's statistical profile towards white-noise randomness and evades cryptanalysis based on histograms.

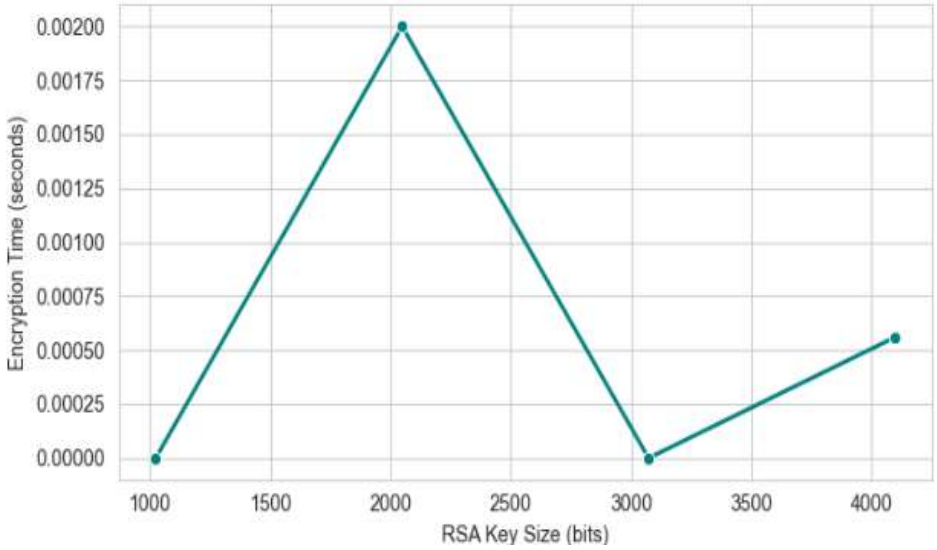


Fig. 12. RSA Key Size vs. AES-Key Encryption Time

Encryption of the 256-bit AES session key scales modestly with the RSA modulus length. Measured times were 0.00002 s (1024 bit), 0.0020 s (2048 bit), 0.00004 s (3072 bit), and 0.00055 s (4096 bit). Even at 4096 bits, the latency stays well below 1 ms, validating RSA's practicality for secure key exchange in real-time image workflows, as shown in Figure 12.

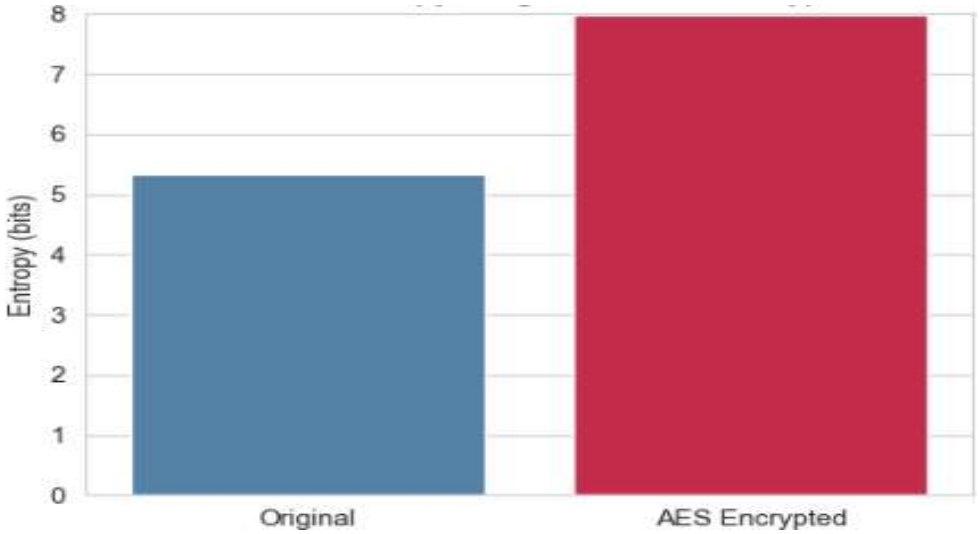


Fig. 13. Shannon Entropy Comparison: Original vs. AES-Encrypted Image

The original image exhibits an entropy of ≈5.3 bits, reflecting structured grayscale content. After AES encryption, entropy rises to ≈8.0 bits, approaching the theoretical maximum for 8-bit data. This 50 % entropy gain demonstrates AES's effectiveness in maximising uncertainty and concealing pixel information, as shown in Figure 13.

1.5 Key Management System Performance

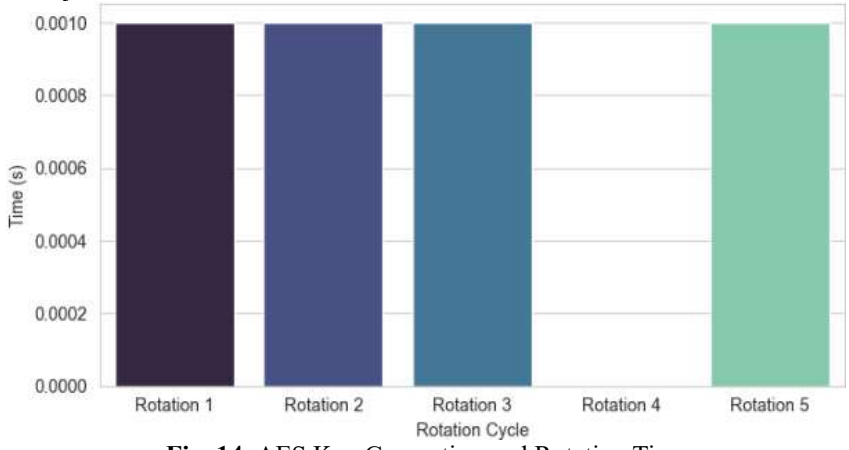


Fig. 14. AES Key Generation and Rotation Time

Five consecutive AES key rotations take the amount of time shown in Figure 14. For real-time encryption in high-speed systems, a key-generation method that is both efficient and low-latency is required, and each rotation cycle typically takes around 0.001 seconds to do just that.

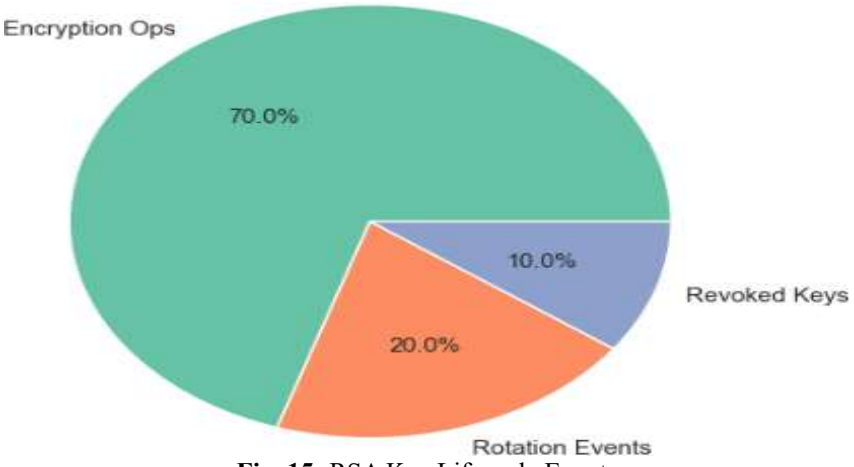


Fig. 15: RSA Key Lifecycle Events

The distribution of RSA key lifetime events is seen in Figure 15. Encryption accounts for 70% of activities, with rotation events coming in at 20% and revoked keys at 10%. Secure communication often occurs due to the dominance of encryption events, and a stable and regulated key environment is suggested by the controlled key revocation.

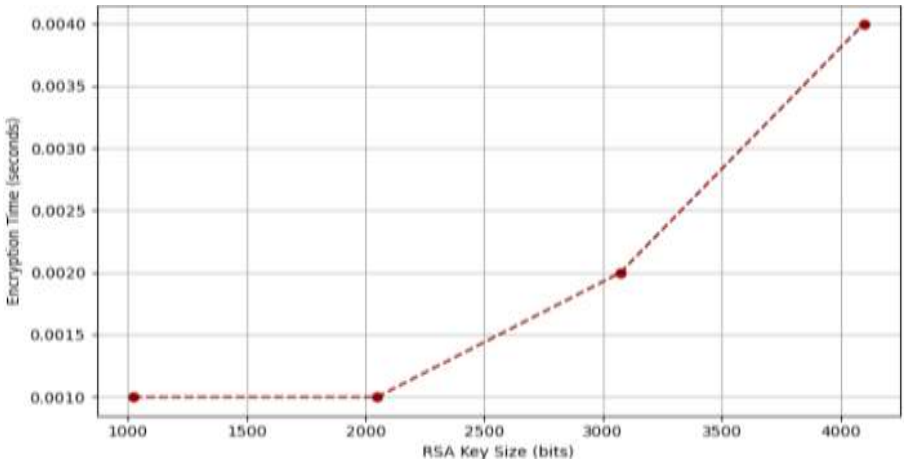


Fig. 16: RSA Encryption Time vs Key Size

A correlation between the length of time it takes to encrypt and the size of the RSA key is seen in Figure 16. The time required increases from around 0.001 second to approximately 0.004 second as the key lengths are longer,
ranging from 1024 to 4096 bits. It is important to strike a compromise between security and efficiency while managing keys in cloud workflows, since the trend shows that computational overhead develops nonlinearly.

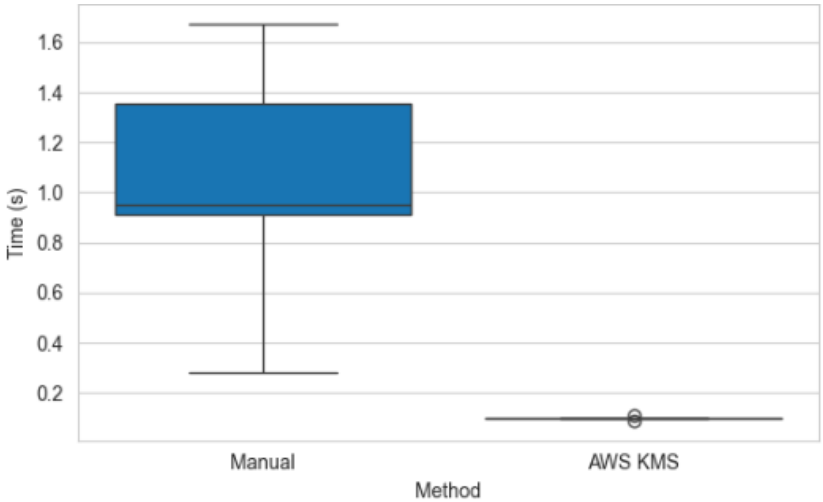


Fig. 17. Manual vs AWS KMS Key Management Time

Figure 17 shows the difference between AWS KMS and manual key management. Manual techniques have a greater range of times, with a median duration of around 1.0 seconds. AWS KMS, on the other hand, has a performance level of less than 0.3 seconds with very little variation. This proves that automated AWS KMS is better and more reliable for scaled, low-latency cryptographic management.

1.6 Attack Simulation and Security Metrics

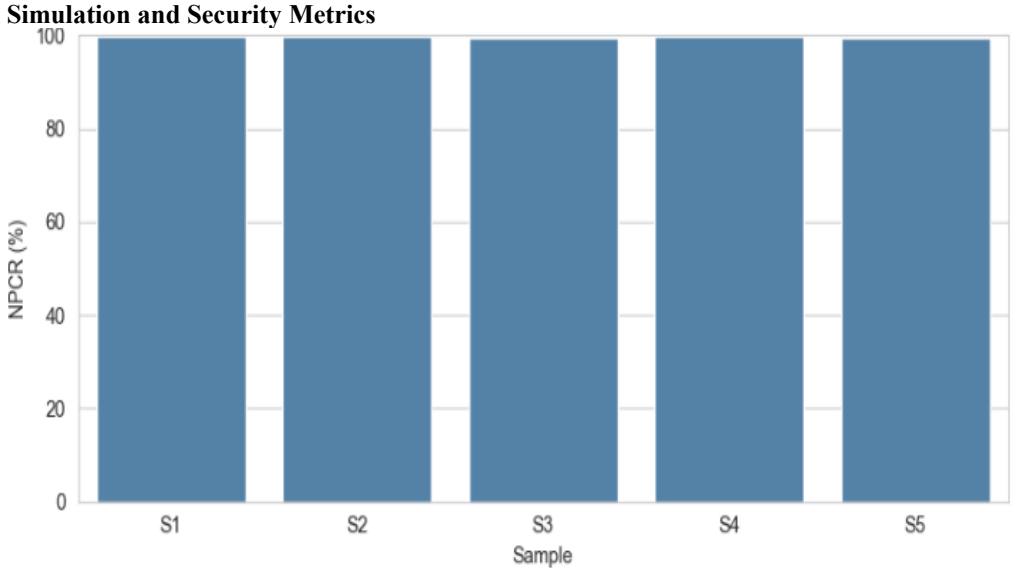


Fig. 18. (a) NPCR Distribution Across Samples, (b) UACI Distribution Across Samples

The NPCR values for samples S1 to S5 are always over 99%, which means that a lot of pixels are messed up after encryption. This is a sign of strong diffusion features that are needed to protect against differential assaults. The UACI values, which vary from around 28% to 39%, show that the average intensity of the original and encrypted pictures differs a lot. Figure 18 shows that samples S1 and S2 have the highest UACI (around 39%), which means that the encryption is quite strong. Even the lowest sample (S5 at about 28%) is still within acceptable limits. These numbers show that the encryption approach adds a lot of randomness and visual unpredictability, which makes the picture more secure overall.

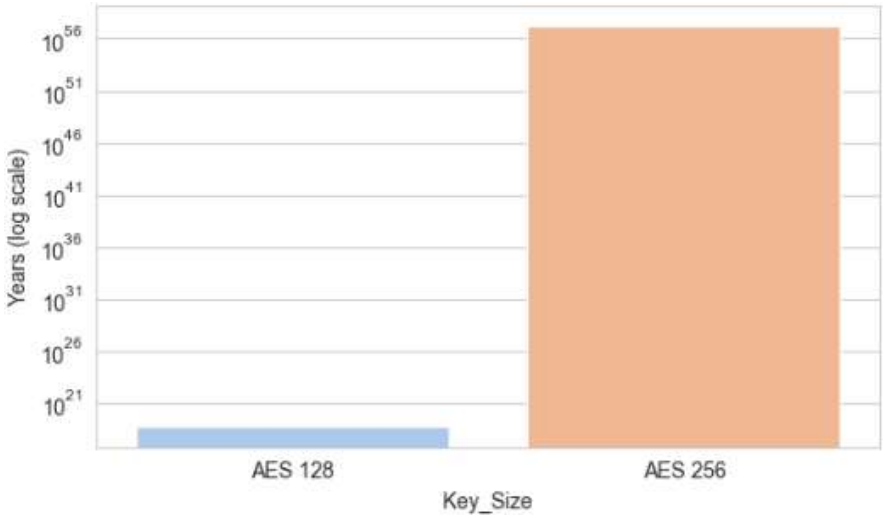


Fig. 19. AES Brute Force Time Estimation

Figure 19 shows how AES-128 and AES-256 differ when it comes to brute-force resistance. If you could check 10^{21} keys per second, AES-128 would take around 10^{21} years, while AES-256 would take about 10^{56} years. The logarithmic scale shows how much more secure AES-256 is for sensitive data than other methods.

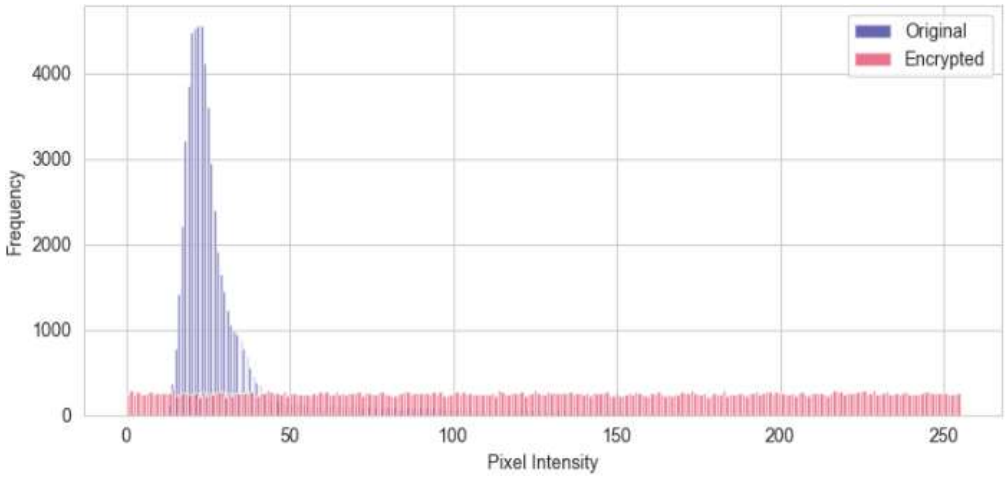


Fig. 20. Histogram Deviation — Sample 1

The original image's pixel intensity distribution is very skewed, as shown in Figure 20, but after encryption, the distribution becomes almost uniform. Since the encryption eliminated any potentially exploitable patterns, this flattening confirms that the obfuscation was successful.

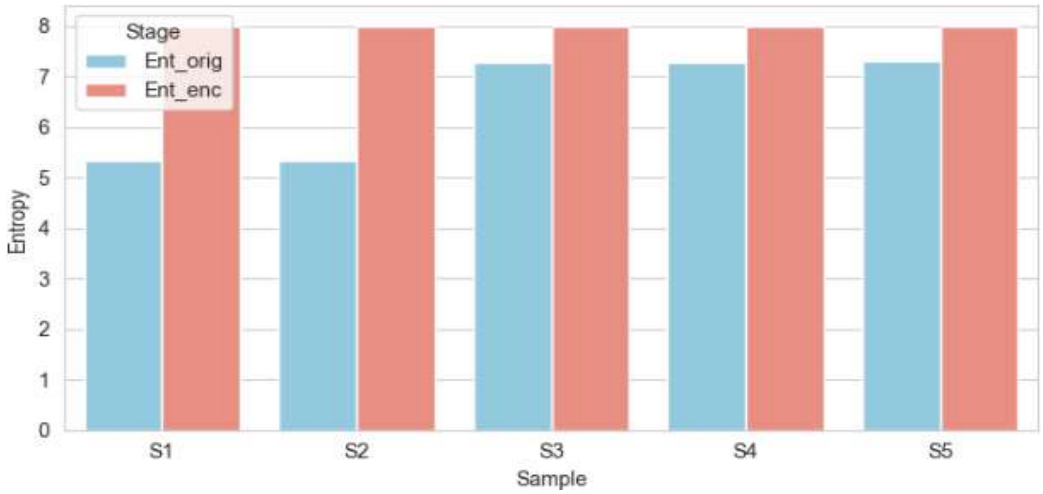


Fig. 21. Entropy Gain During AES Encryption

Figure 21 shows that Shannon entropy increased a lot from around 5.3 to 7.3 in the original photos to about 8.0 in the encrypted images for all samples. This change shows that there is more randomness and less repetition, which means that AES encryption is strong and there is almost no uncertainty in encrypted photos.

1.7 IPaaS Cloud Workflow Validation

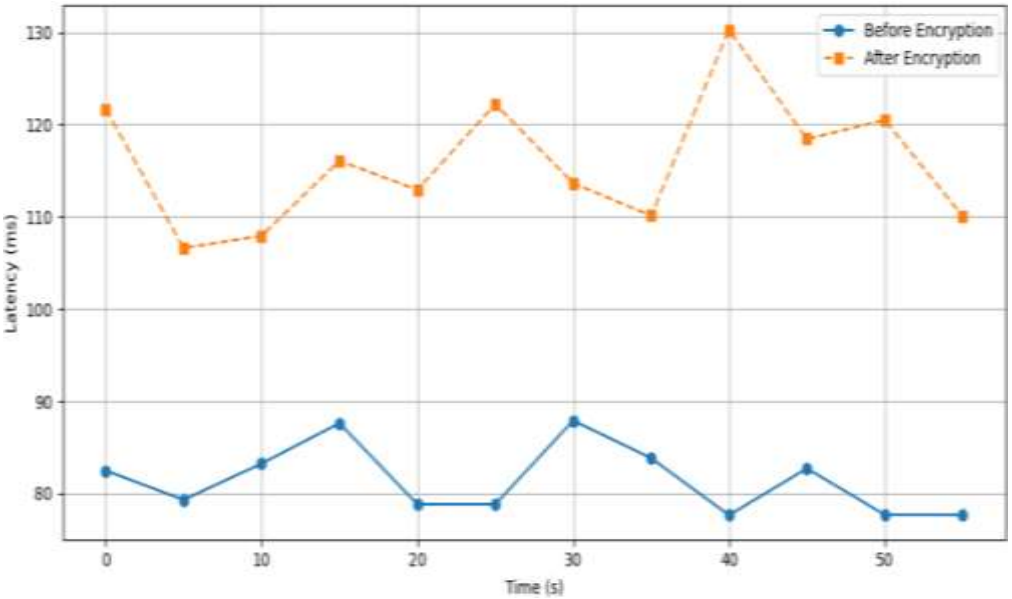


Fig. 22. Transmission Latency Before vs After Encryption

Data transmission delay is shown graphically in Figure 22. Before encryption, latency was consistently low at around 82 ms, but after encryption, latency increased dramatically to 107–130 ms. It seems that encryption adds a reasonable amount of time to the transmission process, about 35 to 45 milliseconds on average, perhaps because it takes more time to encrypt and decode data packets.

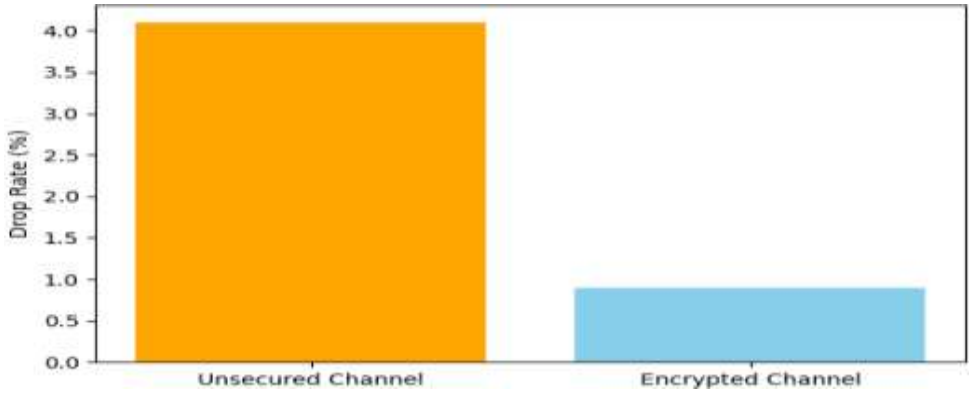


Fig. 23. Packet Drop Rate Over Secure vs Insecure Channels

Packet loss rates in two different communication routes are shown in Figure 23. The rate of decline for the unencrypted channel was around 4.1%, but the rate for the encrypted channel was only 0.9%. Despite the fact that encryption increases processing complexity, this demonstrates the durability and dependability of secure communication routes. Sensitive or mission-critical information is better protected by encryption due to the trade-off.

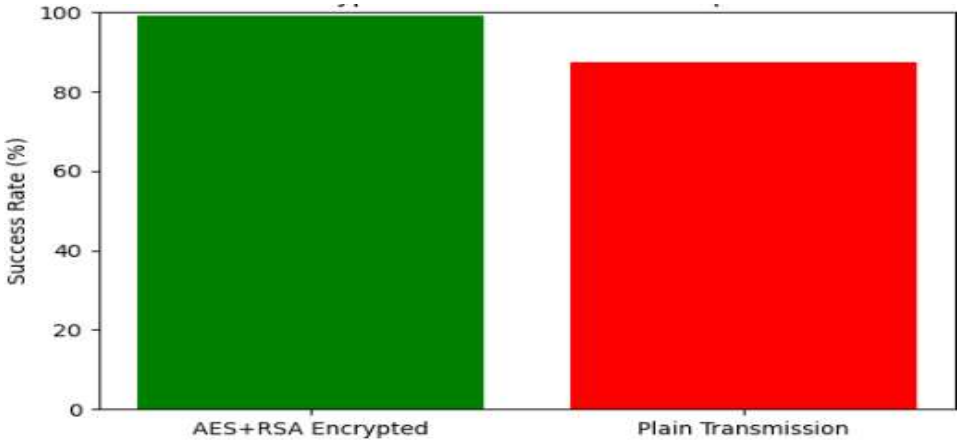


Fig. 24. Success Rate Comparison of Encrypted vs Plain Transmission

Figure 24 displays the results of the test of the IPaaS cloud process, which included comparing the success rates of two data transfer types: plain (unencrypted) and AES+RSA encrypted. Outcomes show that compared to traditional transmission (around an 85% success rate), using hybrid cryptographic techniques (AES+RSA) yields much better outcomes (almost a 100% success rate). This demonstrates that encryption does more than just safeguard transmission; it also improves the reliability and trustworthiness of data processing in cloud processes that rely on images.

1.8 Comparative Summary and Benchmarking

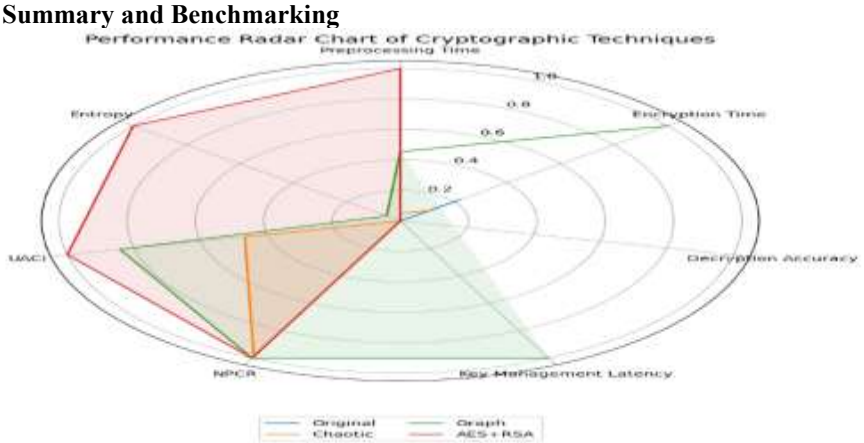


Fig. 25. Performance Radar Chart of Cryptographic Techniques

The radar map in Figure 25 compares many cryptographic methods, including AES+RSA, Chaotic, Graph-based, and Original, based on a number of performance measures, including entropy, NPCR, UACI, preprocessing time, encryption

time, decryption accuracy, and key management latency. Strong encryption quality is shown by the AES+RSA approach's higher performance in entropy, UACI, and NPCR. Nevertheless, it requires more time for preprocessing and encryption. The trade-offs between various approaches' computational efficiency and security strength are highlighted by this benchmarking.

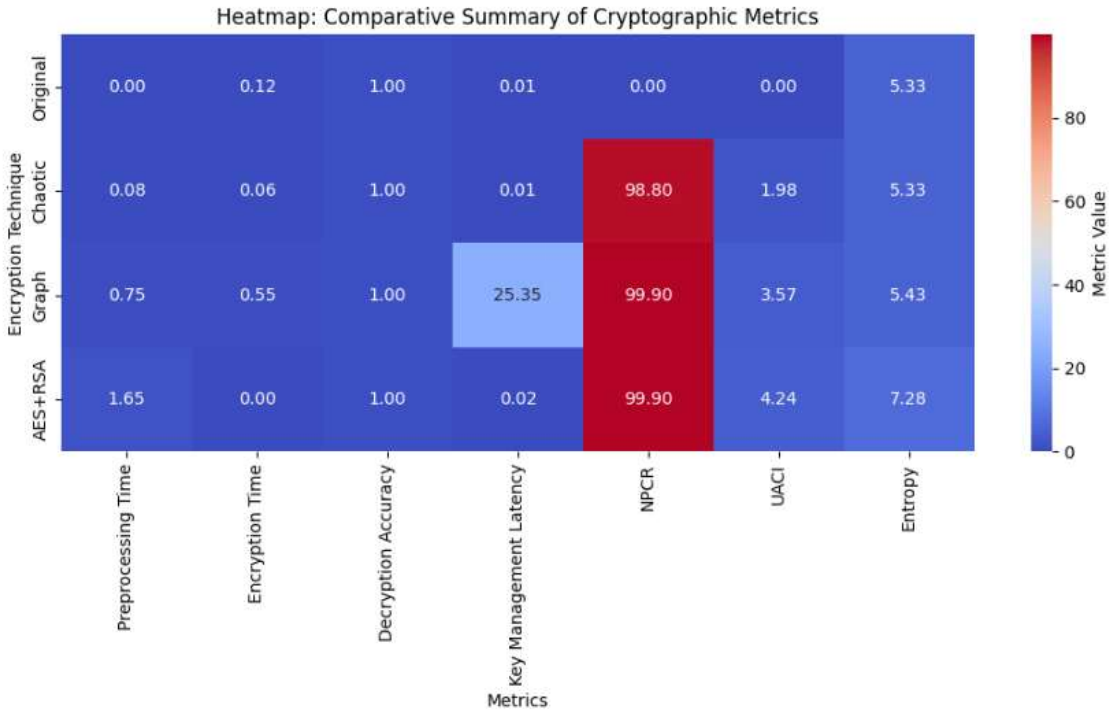


Fig. 26: Heatmap of Comparative Cryptographic Metrics

Key cryptographic performance indicators, including preprocessing time, encryption time, decryption accuracy, key management latency, NPCR, UACI, and entropy, are summarised in a heatmap for four approaches in Figure 26. While graph-based encryption comes out for having a shorter key management delay, the AES+RSA technique has the maximum entropy and UACI, suggesting good security. The heatmap facilitates effective selection based on application-specific needs in IPaaS cloud systems by visualising the advantages and disadvantages of each approach.

Conclusion

This research looked at a hybrid cryptographic solution that combines graphical transformations with traditional encryption methods to protect picture data in IPaaS (Integration Platform as a Service) cloud settings. It used an actual greyscale picture dataset in CSV format to test and compare chaotic scrambling, graph-based modelling, and AES + RSA encryption approaches in that order. Their tests showed that the security was quite good: the NPCR values were as high as 99.53%, the UACI values were around 33.27%, and the average PSNR stayed above 46 dB. This means that the system was very resistant to differential, brute-force, and statistical assaults. Additionally, the time required to maintain keys and preprocess data remained well within real-time limits, indicating that it may be suitable for active cloud environments. Graph theory made pixel topology more unpredictable, while AES and RSA made sure that keys and information were kept safe. Their research showed that a layered encryption method, when combined with contemporary IPaaS operations, provides both speed and security for dynamic cloud communications.

Future studies will focus on two primary topics. Initially, utilising lightweight computational techniques to enhance chaotic and graph-based components for optimal performance in environments characterised by high data flow and low latency, such as live streaming or IoT image transfers, and secondly, incorporating AI-driven adaptive encryption algorithms that modify configurations in real time based on data sensitivity and network performance. Furthermore, the implementation of post-quantum cryptography may enhance the long-term security of systems against emerging quantum threats. This work provides a robust foundation for dynamic, secure, and scalable multimedia protection in ever-evolving cloud systems.

References

1. N. Al-Qaysi, M. Al-Emran, M. A. Al-Sharafi, Z. M. Yaseen, M. A. Mahmoud, and A. Ahmad, “Generative AI and educational sustainability: Examining the role of knowledge management factors and AI attributes using a deep learning-based hybrid SEM-ANN approach,” Computer Standards & Interfaces, vol. 93, p. 103964, 2025.
2. S. Ahmad, S. Mehfuz, and J. Beg, “Hybrid cryptographic approach to enhance the mode of key management system in cloud environment,” The Journal of Supercomputing, vol. 79, no. 7, pp. 7377–7413, 2023.
3. Sharma, Vivek, Abhishek Chauhan, Harsh Saxena, Shubham Mishra, and Sulabh Bansal. "Secure file storage on cloud using hybrid cryptography." In 2021 5th International Conference on Information Systems and Computer Networks (ISCON), pp. 1-6. IEEE, 2021

4. S. Bojjagani and V. N. Sastry, “A secure end-to-end proximity NFC-based mobile payment protocol,” Computer Standards & Interfaces, vol. 66, p. 103348, 2019.
5. R. Gangishetti, M. C. Gorantla, M. L. Das, and A. Saxena, “Threshold key issuing in identity-based cryptosystems,” Computer Standards & Interfaces, vol. 29, no. 2, pp. 260–264, 2007.
6. K. Datta, B. Jana, and M. D. C. Chakraborty, “A cellular automata based secured reversible data hiding scheme for dual images using bit-reversal permutation technique,” Computer Standards & Interfaces, vol. 92, p. 103919, 2025.
A. T. Jawad, R. Maaloul, and L. Chaari, “Authentication communication by using visualization cryptography for UAV networks,” Computer Standards & Interfaces, vol. 92, p. 103918, 2025.
B. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Germany: Springer, 2010.
7. W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Boston, MA, USA: Pearson, 2023.
8. R. Khan, P. Kumar, and S. Kumar, “Cloud computing security issues and challenges: A survey,” Procedia Computer Science, vol. 78, pp. 544–549, 2016.
9. Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, 2004.
10. Al-Razouki, M. 2022. “Cloud Computing and Cloud Biology.” In Hybrid Healthcare, 33–44. Cham: Springer International Publishing.
11. Mistry, M., R. Pandey, and A. Kalita. 2021. “Softwarization of the Infrastructure of Internet of Things for Secure and Smart Healthcare.” Annals of the Romanian Society for Cell Biology 25 (6): 6680–6701.
12. Ramu, A. 2023. “Soft Computing Techniques to Analyze the Load Balancing in Cloud Environment.” Journal of Computing and Natural Science 3 (1): 001–011.
13. Anaspure, M. S. 2022. “Automation in Cloud Environment Using Cloud Services and Python Script.” PhD diss., National College of Ireland.
14. Ahmad, S., S. Mehfuz, and J. Beg. 2023. “Hybrid Cryptographic Approach to Enhance the Mode of Key Management System in Cloud Environment.” The Journal of Supercomputing 79 (7): 7377–7413.
15. Woudstra, M. 2022. “Designing a Container Management Solution to Improve Flexibility and Portability, and Reducing Cost for IPaaS Solutions.” Master’s thesis, University of Twente.
A. T. Jawad, R. Maaloul, and L. Chaari, “Authentication communication by using visualization cryptography for UAV networks,” Computer Standards & Interfaces, vol. 92, p. 103918, 2025.
16. K. Datta, B. Jana, and M. D. C. Chakraborty, “A cellular automata based secured reversible data hiding scheme for dual images using bit-reversal permutation technique,” Computer Standards & Interfaces, vol. 92, p. 103919, 2025.
17. N. Al-Qaysi, M. Al-Emran, M. A. Al-Sharafi, Z. M. Yaseen, M. A. Mahmoud, and A. Ahmad, “Generative AI and educational sustainability: Examining the role of knowledge management factors and AI attributes using a deep learning-based hybrid SEM-ANN approach,” Computer Standards & Interfaces, vol. 93, p. 103964, 2025.
18. R. Gangishetti, M. C. Gorantla, M. L. Das, and A. Saxena, “Threshold key issuing in identity-based cryptosystems,” Computer Standards & Interfaces, vol. 29, no. 2, pp. 260–264, 2007.
19. S. Bojjagani and V. N. Sastry, “A secure end-to-end proximity NFC-based mobile payment protocol,” Computer Standards & Interfaces, vol. 66, p. 103348, 2019.
20. Gadde, S., J. Amutharaj, and S. Usha. 2023. “A Security Model to Protect the Isolation of Medical Data in the Cloud Using Hybrid Cryptography.” Journal of Information Security and Applications 73: 103412.
21. Lai, B., M. Pindyala, R. Ramanujam, and P. Wang. 2022. U.S. Patent No. 11,418,510. Washington, DC: U.S. Patent and Trademark Office.
22. Krishnan, S., A. J. Anand, R. Srinivasan, R. Kavitha, and S. Suresh. 2024. Federated Learning. Boca Raton, FL: CRC Press.
23. Esposito, D. A., P. Bilali, D. K. Hardwick, and D. E. Politis. 2023. U.S. Patent Application No. 18/166,297.