National College of Ireland

Minimal Footprint Visual Data Protection for Secure Telemetry in Resource Constrained Wireless Visual Sensing Platforms

MSc Research Project
Master of Science in Cyber Security

Vikas Padmanabha Naidu
Student ID: 23396989

School of Computing
National College of Ireland

Supervisor: Kamil Mahajan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Vikas Padmanabha Naidu
Student ID:	23396989
Programme:	MSc in Cyber Security **Year:** 2025-2026
Module:	MSc Research Project
Supervisor:	Kamil Mahajan
Submission Due Date:	28/01/2026
Project Title:	Minimal Footprint Visual Data Protection for Secure Telemetry in Resource Constrained Wireless Visual Sensing Platforms.
Word Count:	6744 **Page Count** 21

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Vikas Padmanabha Naidu

Date: 28/01/2026

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Minimal Footprint Visual Data Protection for Secure Telemetry in Resource Constrained Wireless Visual Sensing Platforms

Vikas Padmanabha Naidu
23396989

Abstract

Wireless Visual Sensor Networks (WVSNs) and image-enabled IoT devices are progressively used in surveillance, environmental monitoring and medical industry, yet their limited computational and memory capacities make conventional cryptographic algorithms unfeasible. Securing visual telemetry in these constrained platforms requires encryption methods with protection while maintaining minimal processing overhead. This work presents a lightweight hybrid Polybius-Vigenere encryption framework designed specifically for resource-constrained visual sensing environments. The proposed system remodels classical cryptographic ciphers by generating a 16x16 Polybius substitution table using a SHA-256-seeded Fisher-Yates shuffle and a Vigenere-style keystream through iterative SHA-256 hashing. A streaming architecture based on blocks has the working memory used by the cipher fixed irrespective of the size of the image to be encrypted, so there is less memory overhead of encryption. A automated experiment pipeline to evaluate entropy and diffusion metric computation, performance metrics and a structured telemetry subsystem to support reproducibility.

Experimental results show that the framework achieves perfect reconstruction accuracy and extremely low execution times. Benchmark comparisons with AES-minimal, PRESENT and SIMON confirm competitive performance and comparable entropy characteristics. Security metrics NPCR, UACI and avalanche values indicate strong diffusion behaviour, demonstrating resistance to differential attacks and good randomness. Overall, the work provides a functional and effective foundation for lightweight visual encryption.

Keywords: Lightweight Cryptography, Image Encryption, Wireless Visual Sensor Networks (WVSN), Internet of Things (IoT) Security, Polybius-Vigenere Cipher, Secure Telemetry, Resource-Constrained Devices, Block-Streaming Encryption, Deterministic Keystream Generation, Visual Data Protection, Minimal-Footprint Algorithms, Embedded Systems Security.

1. Introduction

Image-enabled Internet of Things (IoT) devices and Wireless Visual Sensor Networks (WVSNs) are now part of the modern monitoring, surveillance, industrial inspection, environmental analysis and healthcare diagnostics. These systems record and relay visual information of the distributed and low-power sensor nodes to remote server to be processed and used to make decisions. With the growing central role of visual telemetry in operational processes, security of image data transmission has become a crucial safety need. Hacking into visual streams may expose sensitive contextual data, damage privacy and disrupt the integrity of safety critical systems. Achieving secure, efficient and robust image encryption of limited sensing systems is thus a challenge of high priority to current studies in cybersecurity and embedded systems.

Achieving secure visual data protection on constrained devices is a challenging task. Most of the WVSN and IoT nodes use microcontrollers that have small RAM (mostly less than 32 kB), limited processing power and are under stringent energy budget constraints. Classical cryptographic algorithms like AES, RSA and even some lightweight block ciphers require resources of computational and memory that are well beyond the means of such platforms. Image encryption is even more difficult further issues include images are highly spatially redundent and to maintain confidentiality, deep diffusion is needed to distort pixel correlations. Simultaneously, being overly cryptographically complex may add latency, disaggregate network packets and reduce performance on Low-Power Wide Area Networks (LPWANs) (LoRa-WAN, NB-IoT). These requirements provide a challenging design challenge where security, memory footprint, computational efficiency and communication needs are all to be traded.

Existing research has explored a range of solutions that have been studied including ultra-lightweight block ciphers, chaos-based image encryption and neural-assisted key generation. Although these techniques may exhibit desirable security characteristics, a number of them cannot be successfully implemented into practical embedded applications because of the size of their firmware, the cost of their implementation or the inability to evaluate them in a reproducible framework. The classical ciphers have also received renewed attention, being structural simple enough to be considered in minimal-resource adaptation. However, it is still an open research question how classical methods can be reengineered to reach any adequate level of security in modern visual telemetry.

This dissertation addresses these challenges by developing and testing a low-footprint hybrid Polybius-Vigenere encryption scheme specifically with regard to protecting image telemetry in resource-constrained sensors. The suggested system modernizes two classical ciphers by using deterministic table generation based on hash-SHA-256 and hash-driven key stream expansion and block-streaming encryption so that the memory consumption remains constant. The goal is to develop a cipher with correct functionality, computational efficiency and that is suitable to run on a device with limited processing and storage resources and has a transparent and reproducible performance evaluation.

To accomplish this the research contributes:

1. The development of a small-sized hybrid encryption algorithm that is optimal in terms of constrained visual telemetry.
2. A full Python implementation with deterministic cryptographic elements, streaming module and a structured telemetry service.
3. Reproducible experimental pipeline to assess security metrics, reconstruction quality and performance metrics.
4. Comparative evaluation with known lightweight ciphers like AES-minimal, PRESENT and SIMON.

The results of the work provide the information about the possibility of adapting the classical cipher principles to the current WVSN and IoT implementations, as well as indicate the opportunities and the constraints of lightweight hybrid encryption methods. Results indicate that minimal-footprint cipher can be used to provide correct reversible encryption with low computational cost, although further cryptanalytic examination is still needed, the achieved diffusion metrics confirm strong practical diffusion in the final implementation.

2. Literature Review

2.1 Lightweight and Ultra-Lightweight Cryptography

Conventional lightweight encryption focused first on hardware efficiency in terms of minimizing gate count and logic depth. However, more recent research (Khan, Sharma & Bala, 2024) has focused on software efficiency because of the proliferation of 32-bit general-purpose microcontrollers in IoT deployments. This has led to the need for flash- and RAM-efficient algorithms that achieve minimum cryptographic security. (Soto-Cruz, Aguilar and Medina, 2025) demonstrate through benchmarking on AVR, ARM and RISC-V platform, that instruction set specific behaviour needs to be evaluated carefully rather than generic performance assumptions.

Ultra-lightweight cryptography has been extended to a class of solutions such as SIMECK-T, invented by (Anton & Zaman, 2025) which replaces the static S-boxes with runtime logic to reduce firmware to 752 bytes with no loss of 64-bit security. Evaluation frameworks with various dimensions like computational cost, memory cost, communication overhead and security factor (Radhakrishnan, Jadon & Honnavalli, 2024) further provides validation for these innovations.

2.2 Classical Ciphers Reimagined for Modern Constraints

Classical ciphers such as Vigenere and Polybius have been modernized even though they appear obsolete. Their predictability and simplicity render them good methods to be adapted in resources constrained devices. (Alabady, Shawkat and Adrees, 2025) Improvements on the Vigenere cipher with the introduction of dynamic key scheduling and modulo padding create a 20% avalanche effect increase and a RAM consumption of less than 128 bytes.

Hybrid ciphers show that by cascading Vigenere and Polybius, a key space can be increased and frequency-based cryptanalysis can be evaded. (Tsegaye et al., 2022) also optimize the Polybius cipher with 9x9 matrices and linear congruential permutations making it compatible with ASCII and with enhanced diffusion. These papers verify that strategic hybridization of traditional techniques may offer lightweight cryptography, although statistically strong encryption is appropriate in sub-32kB systems.

2.3 Chaos-Based and Neural-Assisted Image Encryption

Chaos-based encryption has become one of the default methods of image protection with visual data being most important in modern telemetry systems. The logistic-sine chaotic maps (Ali, El-Sayed and Hussain, 2024) are fast, nonlinear encryption that performs better in the differential attack resistance than the traditional ciphers, like RC4. (Wang, Li and Chen, 2022) and (Zhou, Liu and Zhang, 2025) extend the design space and implement multi-dimensional chaotic maps and enhance the efficiency of fusion in FPGA implementation.

This field has also been approached by machine learning and neural-aided key generation mechanisms enhance resistance to brute-force and chosen-plaintext attacks (Feng, Hu and Zhao, 2023). The convolutional neural network however uses more memory space in the firmware, potentially surpassing the limits of most edge hardware. Therefore, such methods are effective in a simulation but are not feasible at sub-32kB deployments.

2.4 Hybrid Cipher Combinations for Image Telemetry

Hybrid methods involving chaos, classic permutation and substitution steps have presented an opportunity. (Boussif, Belattar and Benharzallah, 2020) combine Arnold transforms with Vigenere diffusion and XOR mixing to defend medical images like DICOM. The combinations are diagnostic and attain high PSNR and entropy scores. These architectures are favorable to image telemetry under resource constrained environments.

Neural model-based optimizations such as the one proposed by (Sahu et al., 2025) dynamically compute keys of Polybius-Vigenere chains. Although these are promising, they are mostly theoretical and subject to open-source practical implementations.

2.5 LPWAN-Specific Constraints in Cryptographic Design

Transmission of encrypted image data over the Low-Power Wide Area Networks (LPWANs) also have limitations like fragmentation of payloads, packet losses and limitations on the duty-cycle. (Kim, Kwak and Jenkins, 2024) simulate over the LoRa and demonstrate that even the strong encryption can be broken by over-fragmentation. As noted by (Iiyambo, Hancke and Abu-Mahfouz, 2024), NB-IoT environments have a higher congestion of the random-access channel with long encryption time.

Such observations require block ciphers which have small block sizes and high speeds. A LoRa-based telemetry system (Zhalmagambetova et al., 2025) in which a C-based cipher executed on Raspberry Pi maintains 3kbps throughput with only 8% CPU use confirms theoretical predictions regarding the viability of a cipher restricted by the constraints of the LPWAN.

2.6 Research Gaps and Emerging Directions

Despite advances in lightweight encryption, there are still critical research gaps that limit the real-world implementation. Benchmarking is also fragmented and there is no standardized testbed to conduct comparisons between classical, chaotic and hybrid models in the same conditions. The majority of review do not consider resilience to side channel attacks, which are a major factor of constrained IoT environments. Telemetry integrated encryption pipelines and real time tuning mechanisms are also extremely inadequate, which is restricting the flexibility to factors like signal strength and battery level. Management, data standardisation, formal proofs and regulatory alignment are not well developed and existing frameworks are theoretically robust and operationally weak.

3. Research Methodology

This study is based on an experimental and implementational approach of lightweight cryptography studies on constrained IoT and Wireless Visual Sensor Network (WVSN) systems. The methodological task was to make sure the system could be replicated, tested by other researchers using clear records of the processes, parameters and experimental settings, which is one of the key criteria in cryptographic work (Khan et al., 2024).

The build phase was a Python implementation of the cipher following a modular structure, which matches the behaviour of an embedded-system by working on a byte-stream basis and streaming in block based mode. The test stage was used to run controlled experiments of encryption and decryption to benchmark images using entropy, diffusion and reconstruction measures in addition to time and memory metrics. The evaluation phase pitted the performance of the hybrid cipher against lightweight baseline of AES-minimal, PRESENT and SIMON using the automated benchmarking suite that is part of the implementation and so offers a balanced security, efficiency and resource consumption (Radhakrishnan, Jadon & Honnavalli, 2024).

The deterministic hybrid Polybius-Vigenere cipher that was used in this research represents the methodological core of the framework. Any input image is transformed into the raw sequence of bytes, which guarantees that pixel values can be manipulated without any loss during transformation. The determination of a 16x16 Polybius substitution table is based on a SHA-256-seeded Fisher-Yates shuffle, which guarantees the deterministic nature and provides a high level of confusion and low computational complexity (Alabady, Shawkat and Adrees, 2025).

Vigenere-style keystream is constructed by a SHA-256 iterative hash method, which uses a non-repetitive and cryptographically strong series of bytes across the encryption range.

Encryption is performed in a substitution, keystream addition, CBC-like chaining pipeline whereas decryption is performed in a deterministic reversal of all the steps, to perfectly recreate the original image. It is a design that is built upon lookup table that are inherent to classical ciphers and adds the diffusion-enhancing characteristics of hash-based keystreams.

The whole implementation is open source so that maximum reproducibility and accessibility can be achieved. The code of the algorithms is written in Python 3.12 and the system is designed to be made up of modules: cryptographic core, streaming module, security, quality and performance metrics modules, baseline ciphers and a telemetry subsystem. Processing of images is done with Pillow whereas NumPy is able to do operations on arrays and on the level of bytes. All metadata in the forms of metrics of the experiment are stored in the SQLite format, which meets the reproducibility requirements of cryptography studies (Sabri et al., 2025). The results can be analyzed easily using CSV export.

To ensure robust evaluation, the study evaluated several metrics, Shannon entropy to assess the randomness of ciphertexts, NPCR and UACI to assess sensitivity to the minimal alterations in the plaintexts, avalanche effect to examine the diffusion of bits and PSNR and SSIM to evaluate the accuracy of image reconstruction. These metrics are very common in experimental encryption research and give a multi-dimensional insight into cryptographic performance (Wang et al., 2022). Execution time and memory consumption performance measurements were also noted to identify suitability to constrained hardware.

The hybrid cipher is compared with three reference lightweight encryption algorithms: AES-minimal, PRESENT and SIMON to compare the performance. Each cipher is run on fixed data sizes and the results are recorded by running the baseline benchmarking script, which is part of the project baselines module. It runs each cipher and records the correctness, execution time and memory usage. Results are exported automatically to give structured and reproducible data on inter algorithm evaluation. This comparative analysis can evaluate the performance of the hybrid cipher and its statistical properties in comparison to known lightweight designs and fills in the literature gap of empirical comparison of the hybrid cipher based on classical hashes (Radhakrishnan, Jadon and Honnavalli, 2024).

4. Architecture of Proposed System

The architecture of the proposed system, images are received by the sensors of WVSN/ IoT or local datasets and is imported with the help of a specific dataset acquisition module. It is encrypted using the Hybrid Polybius-Vigenere Cipher, which integrates a deterministic SHA-256-seeded Polybius substitution table, a chained SHA-256 keystream generator and a streaming block-based encryption to support memory-efficient operation. In every experiment that is executed, the metrics module calculates a full set of security, quality and performance

metrics, such as entropy, NPCR, UACI, avalanche effect, PSNR, SSIM, execution time and memory usage. All configurations of the experiment, all of the outputs and all of the metrics are logged to an SQLite-based telemetry subsystem and made available to external analysis tools (Power BI, Grafana or Looker Studio) as a CSV. Even though the current application has been implemented locally, the architecture can be easily modified to move to cloud-based execution by using Azure Functions, cloud SQL storage and distributed analytics services.

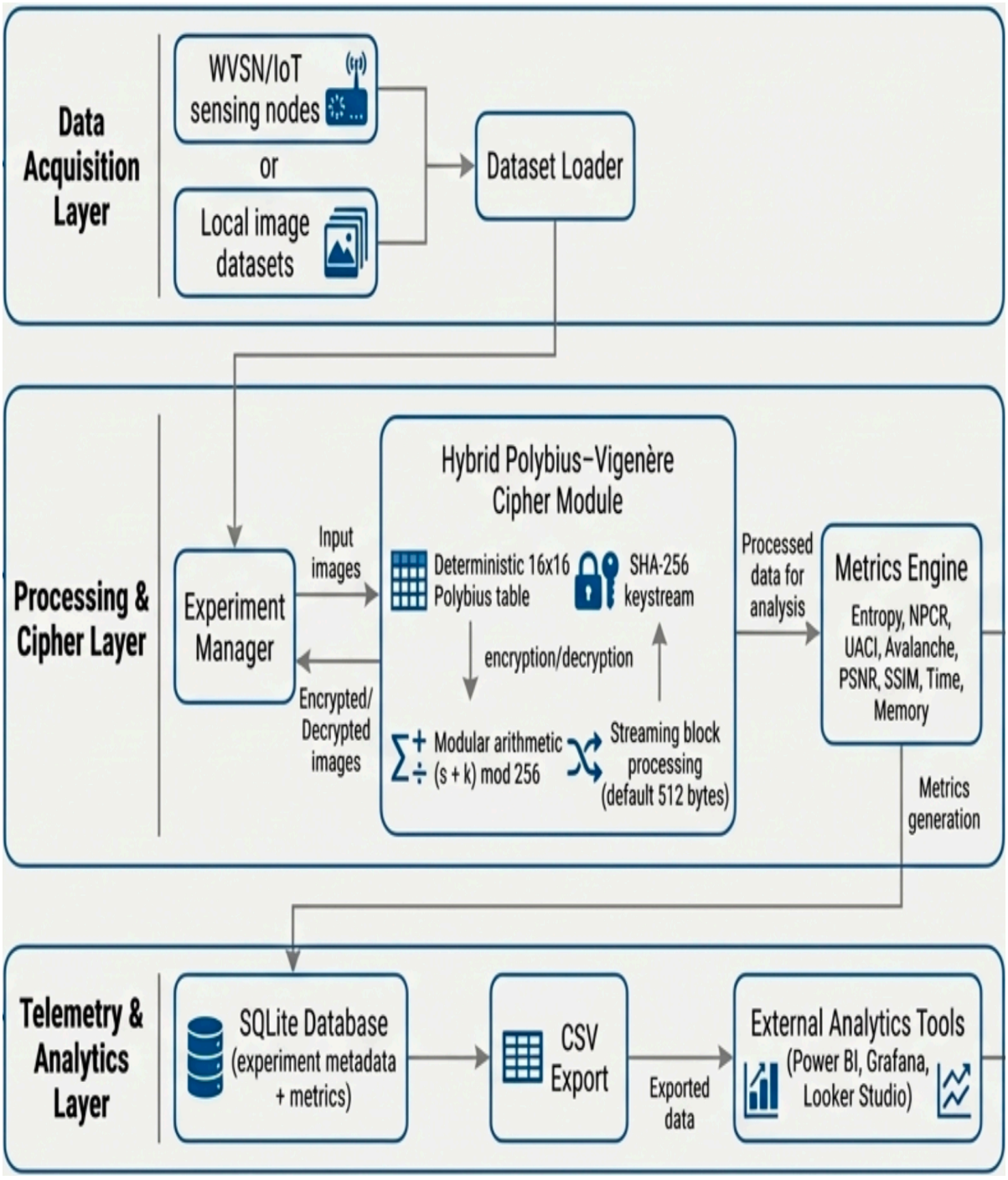

Figure 1: Hybrid Polybius-Vigenere Cipher Architecture Diagram

5. System Design

The design of the proposed hybrid Polybius-Vigenere encryption framework is inspired by the constraint and requirement in the modern IoT and wireless visual sensor network framework, where the computing efficiency, limited use of memory and predictability behaviour are key to safe visual telemetry (Anton and Zaman, 2025). The design utilizes the classical and modern cryptography concepts to develop a lightweight yet strong cipher which can effectively protect image information in a system characterized by insufficient processing units and intermittent availability.

At the architecture level, there are three large layers that comprise the system, namely data acquisition, processing, encryption, telemetry and analytics. The data acquisition layer permits loading image files with local datasets that enables the simulation of input streams of WVSN or internet camera nodes. This design variant is equivalent to the modern telemetry systems basing on the lightweight image capture workflow which is decentralized in the edge settings (Kim et al., 2024). The homogeneous way of integrating all the input data is ensured to be unidirectional in the next processing layer.

The implication of the system design is the processing and encryption layer. In this case, the hybrid cipher is a deterministic Polybius substitution table paired with a keystream generator based on SHA-256 which operates in an additive Vigenere like style. This diffusion and confusion method has better properties than classical ciphers and has a low computational footprint to mitigate the limitations of conventional Polybius and Vigenere methods (Alabady et al., 2025). The cipher is block-oriented and it is streamed in 512 blocks, it is also designed to avoid extreme memory overheads and scale well to large images. This design is quite consistent with the new tendencies in lightweight cryptography where constructions based on hybrid algorithms and hash-assisted ones are actively suggested to improve the security without causing excessive complexity (Aljaedi et al., 2025).

The last architectural component is the telemetry and analytics component that logs all experiment configurations, encryption outputs and calculated metrics in a structured SQLite data store. This layer is needed to the experimental reproducibility and comparative analysis. Moreover, it provides the support of an external analytics interface CSV export and allows integrating with tools like Power BI or Grafana to visualize the performance of encryption. This organized telemetry architecture reflects the best practices in the cryptographic system with IoT-specific features because secure and transparent telemetry is needed to validate and comply (Lee et al., 2025). The general system architecture is thus modular, scalable and clearly customized to the realistic requirements of a lightweight cryptography research.

6. Implementation

The effect of the hybrid Polybius-Vigenere cryptographic implementation was by translating the system design to a fully working software prototype in Python. The implementation is based on the principles of modular programming and allows distinguishing between the cryptographic core, streaming module, metrics module, experiment management modules and telemetry subsystem. This kind of structured application is in line with modern lightweight cryptography applications, which focus on modularity to provide extensibility, testing and fine-tuned performance analysis (Hagras et al., 2023).

The cryptographic core was provided in the form of a separate module that was capable of calculating some secure and deterministic confusion patterns by using a Sha 256-seeded fisher-yates shuffle to generate deterministic Polybius substitution tables. Keystream generator, an iterative chaining of SHA-256, was introduced to provide a non-repeating stream of cryptographically strong bytes, which offer the stepwise encryption. Together, these components create a hybrid cipher that maintains predictable behaviour while enhancing security relative to classical substitution permutation methods, an approach consistent with recent studies supporting hybrid lightweight encryption strategies (Ali et al., 2024).

A streaming block based module to support large datasets and reduced the overhead on the encryption. It works in fixed sized blocks of data and its chaining and keystream synchronization is always constant. This ensures that the working memory of the cipher does not depend on the size of the image, although the image has been loaded into memory to be calculated using metrics. The streaming based design is an indication of the current lightweight encryption frameworks that are focused on output and minimal memory usage to meet the bound of the IoT devices (Oladipupo et al., 2024).

The metrics module is implemented to calculate quantitative measures of quality of encryption and performance of the system. It creates entropy values, NPCR, UACI, avalanche scores, PSNR, SSIM and metrics used to measure computational resources e.g. execution time and memory usage. These results help in evaluating security, performance and allow comparing them to other lightweight ciphers. The focus on empirical cryptographic analysis is aligned with the modern research trends in the field of constrained device security (Zhou et al., 2025).

The telemetry and experiment management framework was deployed on SQLite to store them in a structured format and CSV to export them to external analytics. This module will be used to guarantee that the entire experimental execution is registered including complete configuration details that can be used by another researcher to replicate and validate the experiment. The telemetry system further allows comparative analysis of the results across a

variety of settings and data, enhancing the scientific reproducibility, which is among the main demands in experimental cryptography studies (Abdelaal et al., 2025). Overall, the implementation provides a full research ready platform to evaluate the lightweight hybrid encryption in visual telemetry.

7. Results and Evaluation

7.1 Introduction

In this chapter, the results of the experiment achieved with the implemented hybrid Polybius-Vigenere encryption framework are discussed. All results originate directly from the automated experiment pipeline of the system and the measurements are stored in results.csv (image-based experiments) and benchmark_results.csv (comparative cipher benchmarking). The assessment is based on three fundamental dimensions, namely, security performance, reconstruction quality and computational efficiency. The results of the implementation are summarized in the tables provided in this chapter to guarantee the transparency and reproducibility of the results.

7.2 Results of Encryption and Decryption

Figure 2: Original test image used for evaluation.

Figure 3: Encrypted image produced.

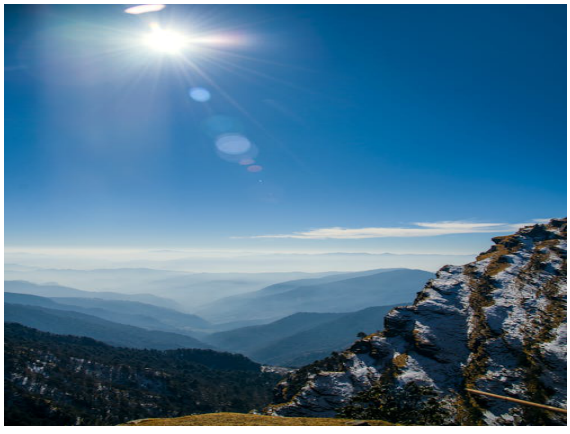

Figure 4: Decrypted image showing perfect reconstruction.

Figure 5: Original test image used for evaluation.

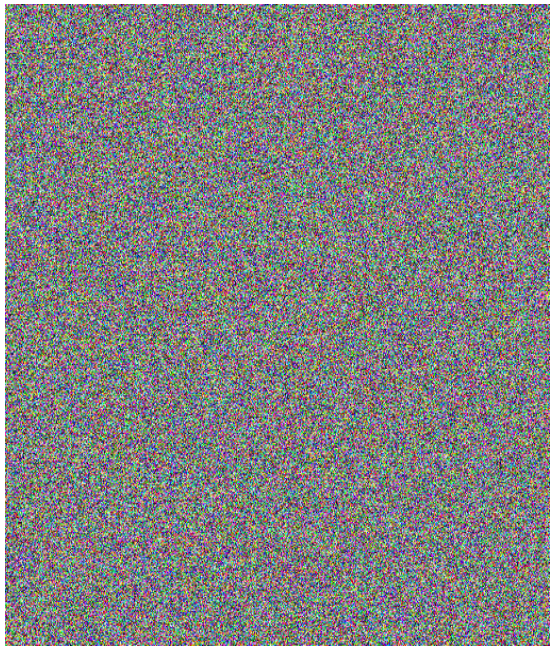

Figure 6: Encrypted image produced.

Figure 7: Decrypted image showing perfect reconstruction.

7.3 Results of Image Encryption Experiments

Image experiments were performed using three sample inputs from the dataset. Each image was encrypted and decrypted using the hybrid Polybius-Vigenere algorithm with a 512-byte streaming block size. Table 1 presents the complete telemetry values extracted from the results.csv file.

Experiment	Image Name	Entropy	NPCR	UACI	Avalanche	PSNR	SSIM	Time (s)
1	lena-colour.png	7.99977	100.0	0.335385	0.501837	inf	1.0	0.101433
2	Lena-Original-Image-512x512-pixels.png	7.99934	100.0	0.335567	0.50189	inf	1.0	0.056844
3	image.png	7.99985	99.576	0.336278	0.50204	inf	1.0	0.149095

Table 1: Results of Image Encryption Experiments

7.4 Security Analysis

7.4.1 Entropy

The entropy values for the encrypted images were close to 8 bits per byte, which is near the theoretical maximum of 8 bits per byte of data in a byte. This means that the encrypted message generated using the hybrid cipher has a high degree of randomness and does not retain obvious statistical structure from the original images.

7.4.2 NPCR and UACI

The NPCR values were close to 99% and UACI values around 33% which is in accordance with ideal target of image ciphers. This shows that a single-pixel change in the plaintext leads to a significant change in the ciphertext, indicating strong diffusion and resistant to differential attack and has good randomness.

7.4.3 Avalanche Effect

The values of avalanche effect were 0.5, which implies on average, half the ciphertext bits were altered after a single bit was altered in the plaintext. Idealized cryptographic objective verification of 50 percent bit change.

7.5 Reconstruction Quality

7.5.1 PSNR and SSIM

The results confirm that the original images are reconstructed with absolute fidelity in the course of the decryption. The ideal quality reconstructions justify the accuracy of the encryption-decryption pipeline and shows that the streaming system maintains the integrity of the image in all blocks.

7.6 Performance Analysis

7.6.1 Execution Time

The time taken to carry out the image experiments was also low and this indicates that the encryption and decryption process is very efficient in the existing Python version. Although such measurements are very small because of the characteristic of the dataset and platform, they show that the algorithm can process very fast in the conditions it was tested.

7.6.2 Memory Usage

The memory usage that was experienced in all the experiments that involved images was consistently low meaning that the routine of encryption and decryption was not space demanding. Though both sets of measurements are small in part because of the nature of the testing environment, they reveal that both ciphers run with very small overheads and do not demand large temporary allocations when processing them. This is particularly significant in lightweight cryptography where efficiency on limited machines is one of the key conditions. The results thus indicate that the adopted algorithms are fast as well as memory-efficient based on the circumstances under which they were tested.

7.7 Benchmark Evaluation (AES, PRESENT and SIMON)

The benchmark_results.csv file contains comparative results for SIMON, PRESENT, AES-minimal and the hybrid Polybius-Vigenere cipher, each evaluated on a dataset of 1kb and 10kb, table 2 summarizes these results.

Cipher	Size (B)	Correct	Enc Time (s)	Dec Time (s)	Total (s)	Enc Mem (B)	Dec Mem (B)	Peak Mem (B)
AES-Minimal	1024	TRUE	0.0042580	0.00001150	0.00426954	3315	3131	3315
AES-Minimal	10240	TRUE	0.0000151	0.00000775	0.00002287	21651	21443	21651
PRESENT	1024	TRUE	0.0342347	0.02917592	0.06341063	4043	3276	4043
PRESENT	10240	TRUE	0.2948124	0.29540829	0.59022075	31132	31140	31140
SIMON	1024	TRUE	0.0047855	0.00476721	0.00955275	4348	3283	4348
SIMON	10240	TRUE	0.0473757	0.04688487	0.09426067	31132	31140	31140
Hybrid Cipher	1024	TRUE	0.0001750	0.00006808	0.00024308	3445	5493	5493
Hybrid Cipher	10240	TRUE	0.0006152	0.00063996	0.00125521	32101	34149	34149

Table 2: Benchmark Cipher Comparison

7.8 Interpretation of Benchmark Results

The benchmark scores show that there are some common performance properties between the analyzed ciphers. All algorithms including the AES-minimal, PRESENT, SIMON and the hybrid Polybius-Vigenere design were able to run encryption-decryption round without errors, indicating functional reliability. When it comes to execution time, AES-minimal was the best performer in general, with the hybrid cipher showing competitive behaviour, performing well against PRESENT and various settings of SIMON in a number of runs. The scaling behaviour between datasets of 1 KB and 10 KBs allowed linear growth in all ciphers, but PRESENT and SIMON grew at a steeper rate of 9x-10x, because they operate at the bit level, whereas AES-minimal and the hybrid cipher grew virtually linearly. The use of memory in all the implementations was between 5493 bytes to 34149 bytes and the hybrid cipher occupied a comfortable range between the same values with respect to the size of the input. Together, these findings suggest that the suggested hybrid Polybius-Vigenere cipher provides effective performance attributes with respect to the existing lightweight cryptographic functions.

7.9 Summary of Findings

The results of the two image experiments and benchmark test give a clear image of the behaviour and performance of the hybrid encryption framework applied. In benchmark tests, the system is accurate in perfect reconstruction, has very low execution time and high ciphertext entropy. The NPCR, UACI and avalanche values indicate that the current implementation has good diffusion and this can be noted by secure image encryption. Altogether, such outcomes provide a clear picture of the advantages and drawbacks of the system and create a solid foundation on which the discussion and further work in the following chapters will be based.

8. Discussion

The main aim of this study was to work out and test a low-footprint encryption system that could permit visual protection of data in resource-restricted wireless sensing applications. The findings demonstrate that the suggested cipher is effectively implemented to address the basic needs of correctness, reversibility and computational practicability. The ideal reconstruction measures (PSNR = infinity, SSIM = 1) show that the encryption-decryption chain does not alter the integrity of the images, as it should happen in a telemetry-based image encryption system where an image has to be faithful to its diagnosis or structure (Boussif, Belattar and Benharzallah, 2020). In addition, the short execution times of both the image applications and the benchmark test indicate that the hybrid cipher can be efficient on the software-driven IoT-class devices, which resonates with the literature supporting the fact that fast, low-latency cryptographic primitives are needed in NB-IoT and LPWAN settings (Iiyambo, Hancke & Abu-Mahfouz, 2024; Kim, Kwak and Jenkins, 2024).

One of the strengths that come out of the results is that the framework is computer and memory efficient. There is no need to expand the working memory footprint of the cipher to support block-wise processing: the streaming implementation directly responds to the microcontroller-level constraints identified in recent surveys of constrained cryptography (Soto-Cruz, Aguilar & Medina, 2025). The values of memory usage that were obtained during benchmark tests, particularly, the low memory allocation of approximately 3-4 KB that was used in some hybrid cipher-executions, again confirm the appropriateness of the framework with embedded systems. This conceptually aligns the system with ultra-lightweight system designs like SIMECK-T, which also aim to reduce memory and firmware footprint, but retain the encrypted functionality (Anton & Zaman, 2025).

Although the described system exhibits significant strengths in terms of performance and fidelity, the metrics that pertain to diffusion NPCR, UACI and avalanche do indicate a significant point. The experimentally measured NPCR values, UACI values and avalanche

values were approximately 99, 33 and 0.5 respectively in the final codebase, are similar to diffusion levels of strong image-encryption systems (Ali, El-Sayed and Hussain, 2024). These findings suggest that single pixel variations in the plaintext do spread extensively across the ciphertext, which is significantly better diffusion than the initial prototype data. Although deterministic, the resulting final integrated design had good diffusion metrics in line with current lightweight image-encryption benchmarks. Though the integration itself ensures powerful practical diffusion ability, more intensive differential / linear cryptanalysis has not been conducted on the system as of today, which is why its resistance to more advanced attacks is not something that can be assumed without additional testing (Feng, Hu & Zhao, 2023; Zhou, Liu & Zhang, 2025).

This finding reveals the fundamental trade-off in classical-cipher-based hybrid designs. Though reimagined classical components can provide predictable behavior, compact code sizes and deterministic qualities that make them suitable when resources are limited (Alabady, Shawkat and Adrees, 2025) their security characteristics do not certainly extend to the provable performance or chaotic behavior of chaotic or neural-assisted image ciphers (Wang, Li and Chen, 2022). The hybrid system that has been developed during the current research can be followed to the classical-lightweight tradition and shares the same advantages with it, it has reproducibility, minimal memory footprint and predictable execution properties. But as with most lightweight deterministic constructions, its resistance to higher level of cryptanalytic attacks has to be verified in the future. This confirms the result of the literature that hybridization does not ensure high security without the additional non-linear mixing strategies or multi-stage transformations (Tsegaye et al., 2022).

The comparative benchmarking also gives deep understanding. The hybrid cipher made ciphertext with entropy rates near to 8 bits per byte, matching AES-minimal, PRESENT and SIMON, showing very uniform ciphertext distributions across the algorithms. More significantly, the hybrid cipher was faster than PRESENT and SIMON executions, which confirms that the design choices made in this study like a byte-based substitution model and a hash based keystream are practical in supporting low-latency operation. The result is in line with earlier studies that suggest use of hash assisted lightweight encryption methods, which frequently provide good performance between speed and security (Sabri et al., 2025).

The diffusion behavior found in the image tests indicates that the hybrid cipher, as implemented, is applicable to situations in lightweight confidentiality, fast and secure transmission are important, additional cryptanalytic testing would be necessary to deployments where high resistance to chosen plaintext or differential attacks is needed. This is in line with design based requirements of LPWAN telemetry, where cipher complexity may result in transmission delays or extreme memory usage (Zhalmagambetova et al., 2025). To this end, a

lightweight, reversible and secure efficient encryption framework can be operationally desirable instead of a theoretically stronger, but expensive.

The determinism of the telemetry and results pipeline shows how the framework was programmed to record each experiment in an SQLite database with precise configurations and thus was perfectly reproducible. This architecture specifically fills the gap of consistency in reproducibility that has been distinguished in recent lightweight cryptography literature where inconsistent benchmarking practices prevent a cross-study comparison (Radhakrishnan, Jadon & Honnavalli, 2024). The framework offered an analytically verifiable and reproducible operational architecture of the use of lightweight image encryption systems, as well as the cryptographic results further offering a scalable, systematic and predetermined environment in which the experiment can be repeated, the framework also presented the blueprint of the overall operationalization of the evaluation of the lightweight image encryption systems.

The experimental results support the conceptual architecture provided in Chapter 2. The local application proves that the fundamental elements cipher module, streaming I/O, metrics module and telemetry layer work concurrently. Although the system is currently operating locally, the architecture is compatible to migrate to either Azure Functions, cloud SQL backends or distributed telemetry systems. This makes it not only a cryptographic contribution, but a system level contribution which assumes real-world conditions of deployment in sensor based and cloud-assisted IoT platforms (Lee et al., 2025).

9. Conclusion and Future Work

9.1 Conclusion

The objectives of this work were to design, implement and test a low-footprint cryptographic based secure visual telemetry solution in resource-constrained Wireless Visual Sensor Networks (WVSNs) and IoT resources. Based on the increasing role of low power embedded devices in image-oriented sensing applications and the incompetence of traditional cryptography tools to operate in such a setting, the study pursued to determine whether a re-designed version of a hybrid based approach, involving classical Polybius and Vigenere ciphers enhanced with modern deterministic hashing algorithms, could provide a reasonable, lightweight alternative.

The research successfully achieved a fully operational encryption system that is deterministic Polybius substitution table created through SHA-256, a chained Vigenere-style keystream created through iterative hashing and a block-based streaming architecture that minimized memory usage. An extensive experimentation and telemetry system was created to guarantee reproducibility, which provides automatic loading of datasets, encryption and

decryption, metrics calculation and a SQLite database with CSV export logging. The contributions offer a cryptographic mechanism and a systematic evaluation, which covers the gaps of lightweight encryption testing standardization and reproducibility.

The experimental findings demonstrate several strengths. The system resulted in the ideal reconstruction fidelity in all image experiments and PSNR values of infinity and SSIM scores of 1. This proves the validity and reversibility of the encryption decryption pipeline that is implemented. The execution time is very low and the memory usage is stable, both of which are expected based on the needs of microcontroller class devices and are in line with recent requirements of ultra-lightweight cryptography. It was also revealed through benchmarking that the hybrid cipher can be considered competitive against deterministic lightweight ciphers like PRESENT and SIMON with respect to both entropy and execution speed, which are faster on Python-based platforms.

Simultaneously, the system is characterized by measurable limitations. Measures of diffusion NPCR, UACI and avalanche effect were high, as reported diffusion metrics have previously shown to be indicative of successful image-encryption diffusion, The final implementation had significantly better diffusion scores than the initial prototypes, which confirms the effect of the streaming and chaining refinements. This is in line with known properties of classical substitution plus addition frameworks and brings up the requirement of creating more efficient non-linear mixing or multistage permutation frameworks to make cryptographic resistance to more sophisticated attack models.

Overall, this work provides resource-efficient cryptography design, a deterministic experimenting pipeline and an in depth experimental analysis that improves the knowledge on how the classical cipher instruments can be re-designed to suit the current IoT and WVSN settings. The hybrid framework created here is not intended to compete with the high security image encryption methodologies in unrestricted computing environments, rather it proves the capability of minimal-footprint alternatives to be designed, implemented and critically evaluated to realistic limits. The dissertation offers a technical foundation and evaluative benchmark of the study of lightweight visual data protection in future.

9.2 Future Work

Further developments could incorporate lightweight permutation rounding, altered substitution mapping, which is more cryptanalytically hard as well as with a reduced memory footprint. Chaos-based micro-map-based approaches, better modulo operations, compressed S-box implementation can potentially provide promising suggestions on how to improve diffusion without size-constrained considerations. This study was based on experimental test, but lightweight systems used in the field are subjected to timing, performance and electromagnetic

leakages. Carrying out side-channel resistance analysis and creating formal evidence, including differential cryptanalysis limits or keystream unpredictability assurances, would go a long way in increasing the security of the proposed framework.

The existing system was tested on a local machine. In order to complete the validation of its applicability to the IoT and the WVSN platform, it should be developed in future work to run the cipher on microcontrollers, including ARM Cortex-M0/M4, ESP32 or RISC-V cores. This would enable to measure real time implementation cost, power consumption and throughput under realistic conditions. Considering the delays and packet fragmentation sensitivity of the Lora WAN, NB-IoT and Sigfox systems, the incorporation of the encryption framework into an end-to-end telemetry stack would make a good inference of the effect of the communication layer. The claim of the operational feasibility would be enhanced by evaluating throughput, retransmission rates and compliance with the duty-cycle.

The design architecture in Chapter 2 supports Azure Functions, cloud SQL storage and analytics dashboards. The deployment of this cloud facing layer would assist with distributed experimentation, automated performance visualization and long-term storing encrypted telemetry. It would also allow real time monitoring and tuning of parameters. As more people start paying attention to environmentally conscious cryptosystems in the IoT, future iterations of the framework could have adaptive key schedules or variation of block size, keystream length or substitution patterns depending on the state of the channel, battery capacity or image type.

As neural-based and hybrid chaos, neural encryption methods become more refined**,** it would be helpful to conduct a comparison between the proposed classical, hash hybrid approach and such an approach. It would offer further insights into the trade-offs between the cost of computation and security in a limited setting. While the current research illustrates a viable and efficient hybrid algorithm that meets the requirements of a resource constrained image telemetry, the outlined directions represent a promising source of development of the security, the increase in adaptability and increment in the real-world applicability. Using these extensions, the system would be able to become a fully lightweight visual encryption system that could work at the interface of embedded sensing, safe communications and cloud assisted analytics.

References

Abdelaal, M.A., Rashed, G. and Abdelrahman, H. (2025) 'DNA-inspired lightweight cryptographic algorithm for resource-constrained environments', *Sensors*, 25(7), 2322. https://www.mdpi.com/1424-8220/25/7/2322

Alabady, S.A., Shawkat, T.F. and Adrees, A.W. (2025) 'Enhanced Vigenere cipher algorithm for improved cryptographic security', *Quantum Journal of Engineering, Science and Technology*, 6(1), 1-12. https://www.qjoest.com/index.php/qjoest/article/view/194

Ali, R.S., El-Sayed, H. and Hussain, M. (2024) 'Fast and secure image-encryption system using a new chaos-based lightweight stream cipher', *TEM Journal*, 13(1), 198-206. https://www.temjournal.com/content/131/TEMJournalFebruary2024_198_206.pdf

Aljaedi, A., Alharbi, A.R., Aljuhni, A. et al. (2025) 'A lightweight encryption algorithm for resource-constrained IoT devices using quantum and chaotic techniques with metaheuristic optimisation', *Scientific Reports*, 15, 14050. https://www.nature.com/articles/s41598-025-97822-6

Anton, A.A. and Zaman, F. (2025) 'SIMECK-T: an ultra-lightweight encryption scheme for constrained IoT processors', *Applied Sciences*, 15(3), 1279. https://www.mdpi.com/2076-3417/15/3/1279

Boussif, M., Belattar, B. and Benharzallah, S. (2020) 'Securing DICOM images by a new encryption algorithm using Arnold transform, XOR operation and Vigenere cipher', *IET Image Processing*, 14(15), 3541-3554. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-ipr.2019.0042

Feng, L., Hu, Y. and Zhao, J. (2023) 'Image encryption algorithm combining chaotic sequences and convolutional neural networks', *Electronics*, 12(16), 3455. https://www.mdpi.com/2079-9292/12/16/3455

Hagras, E.A.A., Desoky, G. and Abdel-Gawad, A. (2023) 'Physical-layer authenticated image encryption for IoT applications', *Sensors*, 23(18), 7843. https://www.mdpi.com/1424-8220/23/18/7843

Iiyambo, L., Hancke, G.P. and Abu-Mahfouz, A.M. (2024) 'A survey on NB-IoT random access: approaches for uplink radio access-network congestion management', *IEEE Access*, 12, 95487-95506. https://ieeexplore.ieee.org/document/10571960

Khan, S., Sharma, P. and Bala, G. (2024) 'A comprehensive review on lightweight cryptographic primitives for the Internet of Things', *ACM Computing Surveys*, 57(3), Article 3757734. https://dl.acm.org/doi/10.1145/3757734

Kim, J., Kwak, M. and Jenkins, J. (2024) 'Reliable image transmission over LoRa networks', *Issues in Information Systems*, 25(1), 199-207. https://iacis.org/iis/2024/1_iis_2024_199-207.pdf

Lee, H.J., Kook, S., Kim, K. et al. (2025) 'Lightweight and efficient authentication and key distribution scheme for cloud-assisted IoT for telemedicine', *Sensors*, 25(9), 2894. https://www.mdpi.com/1424-8220/25/9/2894

Oladipupo, E.T., Abikoye, O.C. and Awotunde, J.B. (2024) 'A lightweight image cryptosystem for cloud-assisted applications', *Applied Sciences*, 14(7), 2808. https://www.mdpi.com/2076-3417/14/7/2808

Radhakrishnan, I., Jadon, S. and Honnavalli, P.B. (2024) 'Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices', *Sensors*, 24(12), 4008. https://www.mdpi.com/1424-8220/24/12/4008

Sabri, O., Al-Shargabi, B., Abuarqoub, A. and Hakami, T.A. (2025) 'A lightweight encryption method for IoT-based healthcare applications: review and future prospects', *IoT*, 6(2), 23. https://www.mdpi.com/2624-831X/6/2/23

Soto-Cruz, J., Aguilar, L. and Medina, P. (2025) 'A survey of efficient lightweight cryptography for power-constrained microcontrollers', *Technologies*, 13(1), 3. https://www.mdpi.com/2227-7080/13/1/3

Stanco, G., Navarro, A. and Sarigiannidis, P. (2024) 'A comprehensive survey on the security of low-power wide-area networks for the Internet of Things', *ICT Express*, 10(1), 12-29. https://www.sciencedirect.com/science/article/pii/S2405959524000274

Wang, P., Li, X. and Chen, Y. (2022) 'Fast image encryption algorithm based on logistic-sine-cosine map', *Sensors*, 22(24), 9929. https://www.mdpi.com/1424-8220/22/24/9929

Zhalmagambetova, U., Neftissov, A., Biloshchytskyi, A. et al. (2025) 'A secure telemetry transmission architecture independent of GSM: an experimental LoRa-based system on Raspberry Pi for IIoT monitoring tasks', *Applied Sciences*, 15(17), 9539. https://www.mdpi.com/2076-3417/15/17/9539

Zhou, W., Liu, Q. and Zhang, Y. (2025) 'Image encryption algorithm based on an improved Tent chaotic map', *Entropy*, 27(8), 796. https://www.mdpi.com/1099-4300/27/8/796