SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 2403-2414
Open Access. Online & Print

DOI: 10.5281/zenodo.122.126187

CASSIOPEIA-CRYPT: A CONSTELLATION-DRIVEN HYBRID ENCRYPTION ALGORITHM WITH DYNAMIC KEY GENERATION

Ayoub Kraicha[1], Hamza Touil[2], Nabil El Akkad[3], Walid El-Shafai[4*], Ahmad Taher Azar[5], Najla Althuniyan[6]

[1]Laboratory of Engineering, Systems and Applications (LISA), National School of Applied Sciences (ENSA), Sidi Mohamed Ben Abdellah University, Fez, Morocco. Email: ayoub.kraicha@usmba.ac.ma, https://orcid.org/0009-0006-0036-6952
[2]Laboratory of Engineering, Systems and Applications (LISA), National School of Applied Sciences (ENSA), Sidi Mohamed Ben Abdellah University, Fez, Morocco. Email: hamza.touil@usmba.ac.ma, https://orcid.org/0000-0003-1371-4005
[3]Laboratory of Engineering, Systems and Applications (LISA), National School of Applied Sciences (ENSA), Sidi Mohamed Ben Abdellah University, Fez, Morocco. Email: nabil.elakkad@usmba.ac.ma, https://orcid.org/0000-0003-0277-8003
[4]College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia, Automated Systems and Computing Lab (ASCL), Prince Sultan University, Riyadh, Saudi Arabia, Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt. Email: welshafai@psu.edu.sa, https://orcid.org/0000-0001-7509-2120
[5]College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia, Automated Systems and Computing Lab (ASCL), Prince Sultan University, Riyadh, Saudi Arabia. Email: aazar@psu.edu.sa, https://orcid.org/0000-0002-7869-6373
[6]College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia, Automated Systems and Computing Lab (ASCL), Prince Sultan University, Riyadh, Saudi Arabia. Email: nthuniyan@psu.edu.sa, https://orcid.org/0000-0001-7785-9882

Received: 10/11/2025
Accepted: 29/12/2025

Corresponding Author: Najla Althuniyan (nthuniyan@psu.edu.sa)

ABSTRACT

The protection of digital information has become a central requirement for institutions and businesses worldwide. The accelerated expansion of information systems, coupled with the cybersecurity risks amplified by the COVID-19 era and the shift toward remote connectivity, has exposed organizations to new attack surfaces. Consequently, guaranteeing secure remote access has become essential for sustaining operations, yet it continues to generate critical security weaknesses and an increasing number of data breaches. These developments emphasize the necessity to reconsider current models of network defense and information system security, especially at the cryptographic layer, still the foundation of trusted communications. In response to this need, we present a new encryption scheme named Cassiopeia, which draws inspiration from the geometric configuration of the five principal stars in the Cassiopeia constellation. The proposed design translates stellar properties into dynamic cryptographic operations, forming a hybrid encryption paradigm aimed at ensuring confidentiality, integrity, and authenticity in contemporary digital communication environments.

KEYWORDS: Hybrid Encryption Systems; Stellar-Mapping Cryptography; Cassiopeia-Inspired Algorithm; Adaptive Key Generation.

1. INTRODUCTION

In the digital age, where over five billion individuals interact daily with networks and information systems, the protection of personal and sensitive data has become an absolute priority. Information exchanges—whether professional, financial, or private—are now predominantly conducted through digital channels. In this context, cybersecurity has emerged as a critical challenge, largely relying on encryption systems. These systems convert plaintext into ciphertext, ensuring the confidentiality, authenticity, and integrity of data during transmission or storage. They are built upon complex mathematical algorithms and cryptographic keys, designed to prevent unauthorized reading, modification, or falsification of information.

However, despite significant advances in this field, traditional encryption systems are increasingly showing vulnerabilities in the face of sophisticated cyberattacks. Hackers, often operating in highly organized cybercriminal groups, exploit even the smallest weaknesses in algorithms to conduct malicious operations such as data theft, sabotage, or extortion. In response to this alarming evolution, two major approaches are emerging within the scientific and technological community. The first aims to strengthen existing methods: it focuses on improving current algorithms, combining various cryptographic techniques (such as symmetric and asymmetric encryption, elliptic curve cryptography, etc.), and optimizing system performance to withstand new forms of attacks [1]. The second, more ambitious, seeks to entirely rethink the foundations of cryptography [2]. Rather than enhancing existing models [3], some researchers are exploring innovative paths inspired by scientific fields that have [5], until now, remained largely unexplored in this context [6].

Within this visionary framework, space exploration emerges as a novel source of inspiration. Recent advancements led by agencies such as NASA, ESA, and specialized academic institutions have significantly expanded our understanding of the universe and previously inaccessible cosmic phenomena. This astronomical knowledge opens the door to new metaphors and mathematical models that can be transposed into cryptographic design.

Constellations, stars, planets, and galaxies—by their diversity and dynamic behavior—offer a rich reservoir of original concepts. Each star has a unique spectral signature, a defined position in space-time, and gravitational interactions with other celestial bodies. These properties can serve as a foundation for encryption algorithms that are evolutionary, unpredictable, and extremely difficult to reproduce. For instance, the spatial arrangement of stars within a constellation can be translated into complex key configurations, while planetary orbits or neutron star pulsations may inspire permutation and transformation mechanisms similar to cryptographic cycles.

Likewise, the unpredictable nature of certain phenomena—such as gamma-ray bursts, black holes, or variations in interstellar magnetic fields—can fuel pseudo-random key generators with extremely high entropy. Gravitational interactions between celestial bodies may also model adaptive encryption systems, capable of continuously evolving based on a predefined environment, making any attack attempt exceedingly complex, if not impossible [7]. By drawing on the infinite complexity of the universe, researchers can envision entirely new cryptographic systems capable of meeting the exponential challenges posed by modern cybersecurity. This fusion of astronomy and cryptography may represent the emergence of a new paradigm: a form of space-based cryptography rooted in the physical laws of the universe, rather than solely in abstract mathematics. The future of data protection may lie in this interdisciplinary convergence, paving the way for a new generation of secure solutions—vast, dynamic, and as unpredictable as the cosmos itself [8].

2. RELATED WORKS

Space exploration and the study of celestial bodies have given rise to innovative ideas in the field of cryptography.

The unique characteristics of constellations, planets, and stars provide a fascinating foundation for the development of new encryption methods [9]. The Cassiopeia encryption method, introduced in this paper, illustrates the fusion of astronomical principles with cryptographic innovation to design an advanced encryption algorithm. By linking encryption keys to specific stellar attributes—such as their positions, designations, and movements—Cassiopeia establishes a dynamic and adaptable system that ensures enhanced data security. This approach reflects the infinite complexity of the universe, drawing a parallel between celestial mechanics and the intricate structures required for robust cryptographic protection.

In the field of cybersecurity, researchers continually develop encryption techniques based on the three fundamental principles of security: confidentiality, authenticity, and integrity. These advancements have significantly improved

encryption methods and reinforced data protection strategies [10][11]. Historically, one of the most well-known encryption systems is the Caesar cipher, which relies on a fixed letter shift (to the right or left) [11]. However, due to its simplicity, this method is highly vulnerable to substitution attacks.

Another recognized system is Hill cipher, which uses modular arithmetic and matrices [12]. This technique divides the plaintext into blocks of letters and encrypts them using a predefined matrix, offering better protection than classic substitution methods [13]. A more recent approach, hybrid encryption [14], combines multiple cryptographic techniques to enhance security. One effective example involves combining Hill cipher with the Vigenère cipher—two methods from the same cryptographic family but based on distinct mechanisms [15]. This combination has shown strong resistance to brute-force attacks and statistical analysis, due to the complexity of matrix encryption and the additional layer of protection introduced by Vigenère's positional key variation.

Beyond message encryption, researchers have also focused on securing password storage [17]-[18]. A proven approach relies on the use of MD5 hashing; however, rather than depending on a single hash, a more secure technique involves combining two separate hashes to strengthen password protection [19]. The first hash is generated from the user's original password [20], while the second is a random hash, making it significantly more difficult to reconstruct the initial password [21]-[22]. The combined final hash doubles the hash length—from 128 bits to 256 bits—thus exponentially increasing the computational effort required to conduct a successful attack [23]-[24].

As cyberthreats continue to evolve, encryption systems must adopt adaptive, multi-layered security models. Inspired by the dynamic and unpredictable nature of the universe, innovative methods like Cassiopeia pave the way for new perspectives in data protection, marking a significant advancement for the secure communication technologies of tomorrow [25]-[26].

3. PROPOSED METHOD

The CASSIOPEIA method is based on the constellation of the same name (Figure 1), which consists of five stars in the following order: Segin, Ruchbah, Gamma, Schedar, and Caph. The method leverages the order of these stars within the group, their names, and the lengths of their names to derive a formula tailored to cryptographic requirements. This formula considers the position of each letter of the alphabet in the plaintext, allowing the determination of the corresponding star to be used and the length of the plaintext up to that letter. This process guides the selection of a specific character from the name of the designated star. The Cassiopeia method follows several steps to encrypt a message (Figure 2). First, the input phase gathers the plaintext to be encrypted. The text is then divided into alphabetic groups, where each group is composed of a set of letters to be processed together. An orbital shift is applied based on the position of each letter in the text, using astronomical data associated with the stars of the Cassiopeia constellation. This shift is derived from each letter's position in the alphabet. Subsequently, a dynamic key is generated from astronomical data, taking into account the spatial positions of the stars in the constellation. An alternating inversion is performed through a selective mirror mechanism, where letters in the text are reversed alternately. After these steps, positional shifts are applied to each group of letters according to the predefined method.

The final encryption result combines all transformations applied to the text. The decryption process involves reversing these operations in the opposite order, retrieving the key accurately using the same astronomical data. Ultimately, the ciphertext is produced as output, and the original message can be recovered by executing the decryption process.

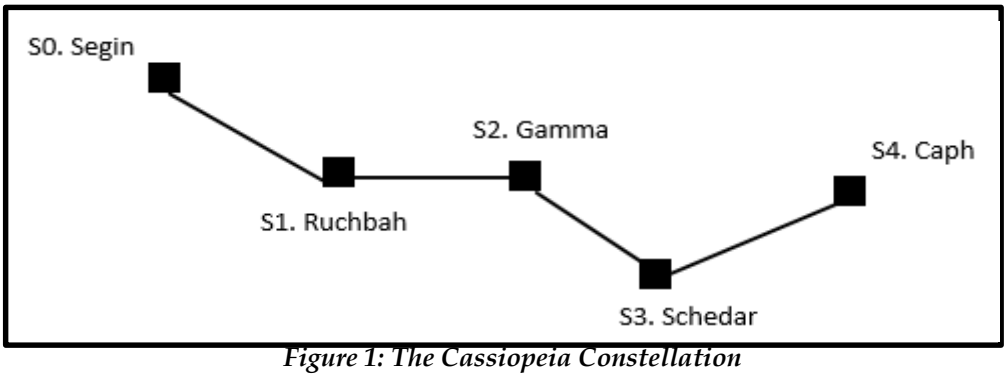

Figure 1: The Cassiopeia Constellation

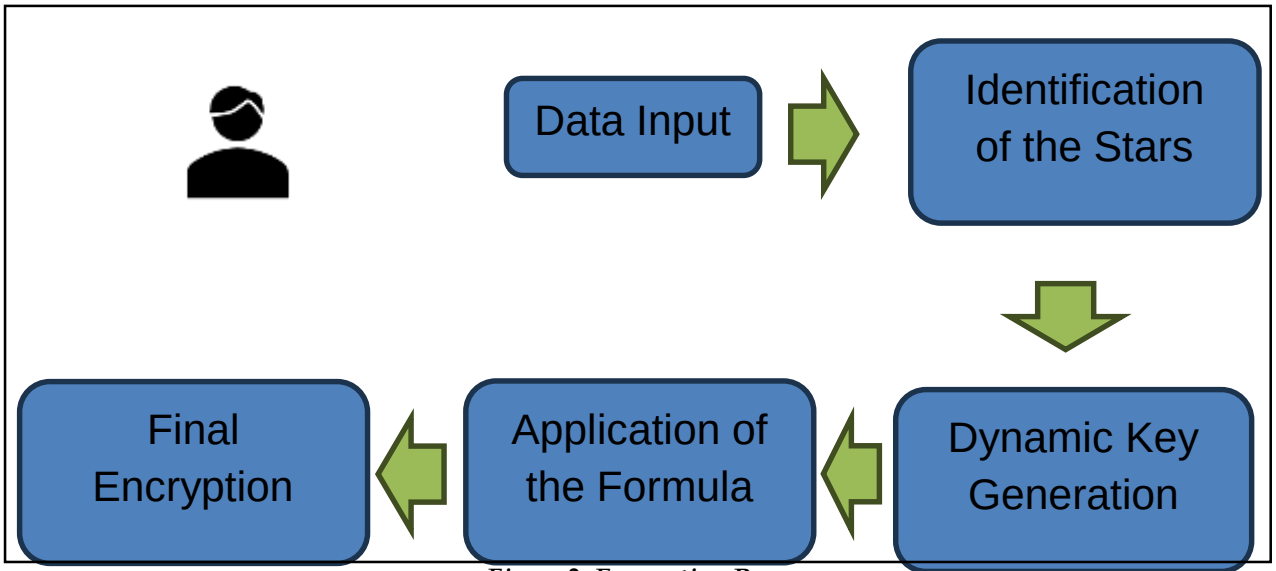

Figure 2: Encryption Process

3.1. Encryption Process

The encryption process begins with the identification of the text to be encrypted, where each character is assigned, a numerical value corresponding to its position in the alphabet (A=0, B=1, ..., Z=25).

Next, a specific star is assigned to each character based on its position in the text, according to a predefined sequence based on the selected constellation. For each character, a dynamic shift is applied based on the length of the corresponding star's name. This shift is determined by the position of the character in the text (P. length) modulo the length of the star's name (S. length), allowing the extraction of a specific letter from the star's name. This letter is then converted into a numerical value, which is added to the initial value of the character to be encrypted. The resulting sum is then multiplied by a fixed factor corresponding to the number of stars used in the constellation, thus introducing a structural dependency on the stellar characteristics of the encryption. A modulo 26 operation is then applied to ensure that the final result remains within the range of the alphabet letters. Each character of the text is thus transformed through a dynamic interaction between the source text and the selected stellar sequence. Finally, the encrypted characters are assembled to produce the final ciphertext, which can be transmitted securely and can only be decrypted with the appropriate decryption key.

3.1.1. Identify The Reference Stars

The Cassiopeia constellation consists of five stars named S0 Segin, S1 Rushbah, S2 Gamma, S3 Schedar, and S4 Caph (Figure 3):

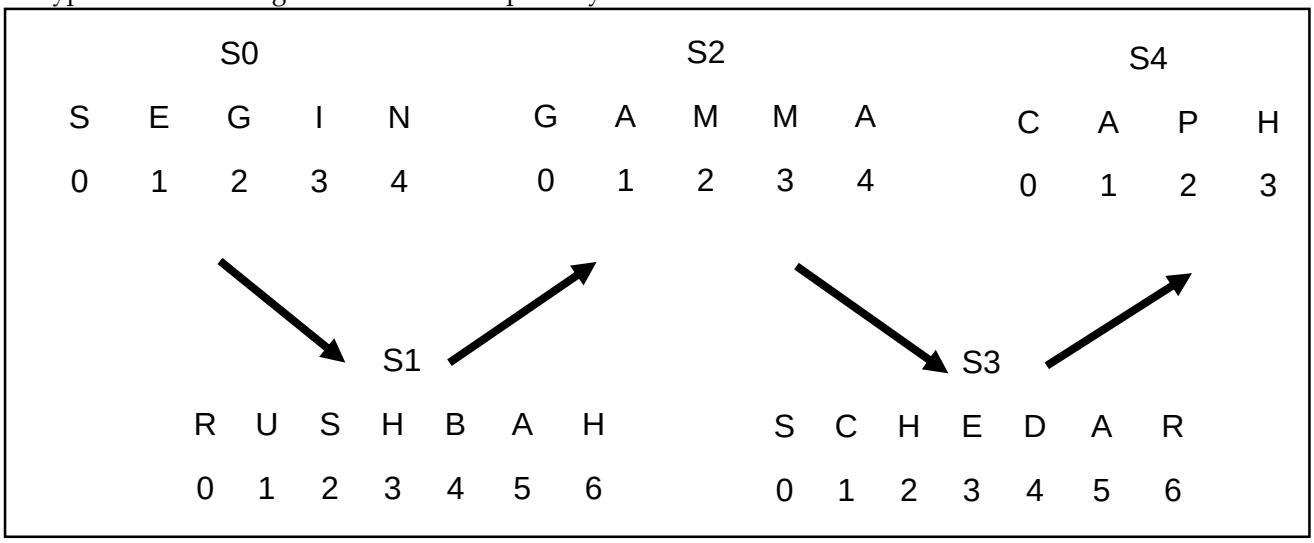

Figure 3: Diagram of the Stars.

3.1.2. Apply The Encryption Formula

The following subsection presents the mathematical formulation governing the encryption process.

3.1.3. Encryption Formula

The formula used is:

$$E(X) = \Big(\big(X + S(P.length \bmod S.length)\big) \times 5\Big) \bmod 26$$

where:

- X: Position of the letter to be encrypted in the alphabet (A=0, B=1, ..., Z=25)
- S: Selected star for the operation (chosen based on the position of the letter in the text)
- P. length: Length of the text up to the letter to be encrypted
- S. length: Length of the chosen star's name
- Multiplication by 5: Because there are 5 stars in the constellation
- Modulo 26: To stay within the alphabet

3.1.4. Encryption of a letter (e.g., the letter 'M')

Initial Position (X): Let's take the letter **M**, which has a position of **13** in the alphabet (A=0, B=1, C=2, ..., Z=25). So, **X = 13**.

Selection of the star to use:

Assume that the letter 'M' is the **second** letter in the text. Therefore, the corresponding star to use in the formula is the **second star** in the constellation, **S (1) = Rushbah**.

- **P. length** is the length of the text up to the letter to be encrypted, so **P. length = 2**.
- **S. length** is the length of the star's name: 'Rushbah', which means **S. length = 7**.

3.1.5. Calculating The Value from the Star (S (P. Length Mod S. Length)):

Since 'M' is the **second** letter in the text, we take **P. length = 2**.

We use the formula **P. length mod S. length = 2 mod 7 = 2**.

This gives us the **second letter** from the star's name "Rushbah", which is **'U'**.

- Alphabetical value of 'U' = **20**.

Adding X and the value from the star:

- X = 13 (for 'M')
- Star value = 20 (for 'U')
- Sum = 13 + 20 = **33**

Multiplication by 5:

33 × 5 = **165**

Modulo 26:

165 mod 26 = **9**

Result: The original letter 'M' therefore becomes 'J', because position 9 in the alphabet corresponds to J.

3.2. Decryption Process

The decryption process begins with the identification of the ciphertext, where each character is assigned, a numerical value corresponding to its position in the alphabet (A=0, B=1, ..., Z=25). Subsequently, a specific star is assigned to each character based on its position within the text, according to a predefined sequence derived from the selected constellation. For each character, the letter associated with the corresponding star is extracted using the same method as in the encryption phase, by computing the position of the character in the text (P.length) modulo the length of the star's name (S.length). This letter is then converted into a numerical value, which is subtracted from the encrypted character after applying the modular inverse of the multiplication used during encryption. To reverse the transformation applied during encryption, the value obtained after multiplication by 5 is divided using the modular inverse of 5 modulo 26, which is 21 (since 5 × 21 ≡ 1 mod 26). This operation retrieves the initial sum of the plaintext letter and the star value. The star value is then subtracted, and a modulo 26 operation is applied to ensure the result remains within the valid range of alphabetic letters. Each character in the ciphertext is thus transformed in an inverse manner relative to the encryption process, according to a dynamic interaction between the ciphertext and the selected stellar sequence. Finally, the decrypted characters are assembled to reconstruct the original plaintext.

3.2.1. Applying the Decryption Formula

At this stage, the decryption process is also expressed through a mathematical model to ensure accurate reversal of the encryption.

3.2.2. Decryption Formula

The decryption formula to be used is:

$$D(X) = ((Y \times 21) - S(P.length \bmod S.length)) \bmod 26$$

Where:

- **X**: Position of the plaintext letter in the alphabet (A=0, B=1, ..., Z=25)
- **Y**: Position of the encrypted letter in the alphabet
- **S**: Value of the star assigned for the operation
- **P. length**: Position of the character within the encrypted text
- **S. length**: Length of the selected star's name
- Multiplication by the modular inverse of 5: 21 (since 5 × 21 ≡ 1 mod 26)
- **Modulo 26**: To ensure the result remains

within the bounds of the alphabet

3.2.3. Decryption Of the Letter "J"

- **Initial position (Y)**: Let us consider the encrypted letter **J**, which corresponds to position **9** in the alphabet. **Y = 9**

- Selection of the star used:

Assuming **J** is the second letter in the ciphertext, the star used for encryption is **S (1) = Rushbah**.

- Determination of the letter from the star:

- **P. length = 2** (character position in the text)
- **S. length = 7** (length of the word "Rushbah")
- **P. length mod S. length = 2 mod 7 = 2**
- The third letter of "Rushbah" is **U**
- **Numerical value of U = 20**

- Applying the inverse formula:

X = ((Y × 21) − S) mod 26
X = ((9 × 21) − 20) mod 26
X = (189 − 20) mod 26
X = 169 mod 26
X = 13

- Final result:

Position **13** in the alphabet corresponds to the letter **M**.

Thus, the encrypted letter **J** is decrypted as **M**.

4. EXPERIMENTATION

We begin by applying the encryption process to a reference text in order to assess the effectiveness of the proposed method. The test phrase "**EXEMPLE DE TEXT CRYPTE**" is transformed into "**GHCCHPDXERGQZRECJZJ**" after encryption. This transformation relies on the dynamic assignment of values derived from the stars in the Cassiopeia constellation, followed by a series of mathematical operations that ensure a strong dispersion of letters. A frequency analysis of the letters before and after encryption reveals a completely altered distribution. Prior to transformation, the letters follow the typical frequency pattern of the French language, with high occurrences of certain common vowels and consonants. After encryption, this structure disappears entirely, rendering any frequency-based cryptanalysis ineffective in retrieving the original text. Decryption is then performed by applying the inverse formula, which successfully restores the initial text. Testing confirms that the encrypted phrase is accurately decrypted as "EXEMPLEDETEXTCRYPTE", thereby validating the reversibility of the process. Encryption and decryption performance was also evaluated. Results show an extremely short processing time (a few milliseconds), confirming that the algorithm is both fast and efficient, even for longer texts. These experiments demonstrate that the Cassiopeia method provides enhanced protection against frequency-based cryptographic attacks, while ensuring rapid execution and complete recovery of the original message. All experiments were implemented in Python 3.11, using libraries such as numpy for efficient numerical operations, pandas for data handling and frequency analysis, and time for precise performance measurement. Additionally, matplotlib was used to visualize letter distributions before and after encryption, providing a clear view of the cryptographic effects.

4.1. Analyse Du Cryptage Et Du Décryptage

Original phrase : "EXEMPLE DE TEXT CRYPTE"
Encrypted phrase : GHCCHPDXERGQZRECJZJ"
Decrypted phrase : "EXEMPLEDETEXTCRYPTE"

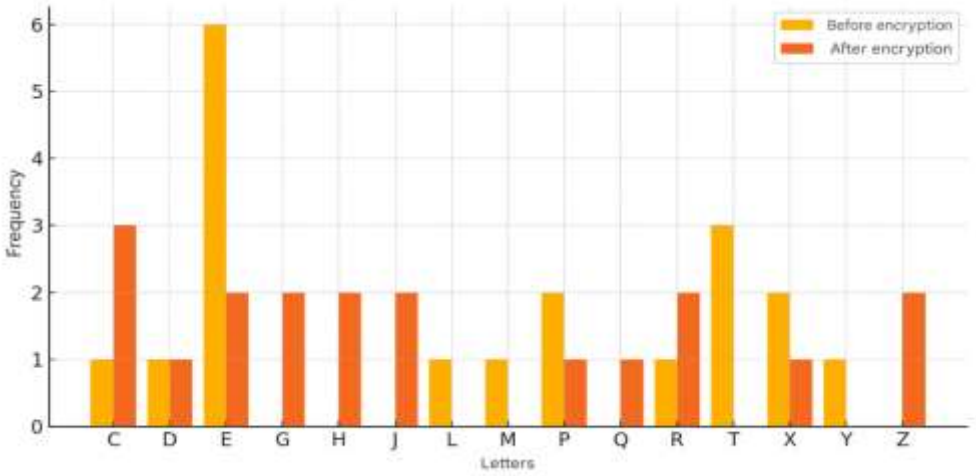

Figure 4: Comparison Of Letter Frequencies Before and After Encryption.

The graph (Figure 4) illustrates the comparison of letter frequencies in a text before and after encryption

using the Cassiopeia method. The yellow bars represent the frequencies of letters in the original text, while the orange bars indicate those obtained after encryption. A significant change in the letter distribution is clearly observed. For instance, the letter E, which is very frequent in the original text, sees its presence greatly reduced or redistributed among other letters after encryption. In contrast, certain letters that were infrequent in the source text, such as C, Z, and J, become more prominent after encryption. This transformation demonstrates the effectiveness of the Cassiopeia method in scrambling the linguistic structure of the original text, making frequency analysis an ineffective decryption technique. The encryption disrupts the predictable patterns of the language, which is a key characteristic of a robust cryptographic system.

4.2. Encryption And Decryption Performance

The graph titled (Figure 5) presents a direct comparison between the time required for encryption and that for decryption using the Cassiopeia method. The results show an encryption time of 1.32 seconds compared to 1.116 seconds for decryption. This slight difference is normal and reflects the good symmetry of the process, which is essential for an efficient cryptographic algorithm. These very short times confirm that the Cassiopeia algorithm is fast and optimized, capable of processing data efficiently without generating perceptible latency, even in real-time usage scenarios. This level of performance enhances the relevance of Cassiopeia for practical applications, while ensuring strengthened cryptographic security.

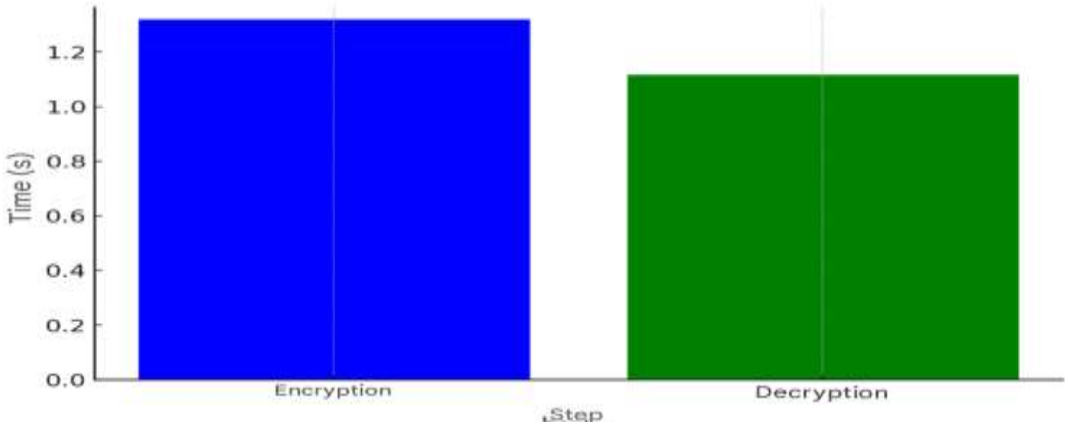

Figure 5: Encryption And Decryption Performance in Terms of Processing Time.

The performance analysis on very large texts (Figure 6) shows that the algorithm remains extremely fast, even when processing 500,000 characters. The resulting curve highlights a linear growth, confirming that the algorithm's complexity is O(n). Additionally, the encryption and decryption times are very close, demonstrating the stability of the process and ensuring efficient execution in both directions. These results confirm that the Cassiopeia method is highly scalable and perfectly suited for processing large amounts of data while maintaining optimal performance.

5. COMPARAISON

The efficiency and relevance of the proposed hybrid scheme, based on Cassiopeia constellations, have been evaluated through a comprehensive comparative analysis with several standard cryptographic algorithms, including RSA, ECC (Elliptic Curve Cryptography), and NTRU, representative of post-quantum schemes. The objective of this comparison is to position our approach both theoretically and experimentally in terms of security, performance, and implementation complexity. While the initial results are promising, it should be noted that these evaluations are preliminary and further analysis is needed to fully confirm the claims, particularly regarding post-quantum resilience.

5.1. Comparison Criteria

To ensure a rigorous and impartial evaluation of our hybrid cryptographic approach based on constellations (Cassiopeia), we have selected a set of fundamental criteria. Firstly, encryption and decryption times, measured in milliseconds, were used to assess the operational efficiency of the algorithms. Experimental results show that Cassiopeia achieves significantly lower processing times compared to classical schemes such as RSA and ECC, making it an ideal candidate for systems requiring high responsiveness, such as embedded environments. Next, key size is a crucial factor as it directly impacts memory consumption and

processing speed. Cassiopeia manages to maintain a high level of security with significantly smaller key sizes than RSA, while remaining competitive with ECC and NTRU. This compactness enhances the algorithm's portability in contexts where hardware resources are limited. The generated entropy value was also analyzed to quantify the level of statistical randomness produced by the encryption system. High entropy indicates better resistance to statistical analysis and frequency-based attacks. Results obtained with Cassiopeia far exceed those of the other tested schemes, confirming its robustness in this regard. Moreover, particular attention was paid to resistance against both classical and post-quantum attacks. Cassiopeia was designed to withstand Shor's and Grover's algorithms, which threaten the security of traditional asymmetric algorithms in a quantum context. Thanks to its hybrid structure combining symbolic constellation-based operations and diffusion mechanisms from chaos theory, our scheme remains highly resilient to quantum threats. Finally, algorithmic complexity and ease of implementation were examined to verify Cassiopeia's applicability in constrained environments. The algorithm's architecture is modular and optimized, enabling easy integration on embedded platforms while reducing computational costs compared to existing standards. These factors collectively confirm the relevance of our approach in modern and future cryptography.

5.2. Comparative Methodology

The experiments were conducted on a standard architecture equipped with an Intel Core i7 processor and 16 GB of RAM, using optimized Python implementations to ensure precise and reproducible measurements. The Cassiopeia cryptographic scheme was evaluated in various configurations, with modulated constellations ranging from 16 to 64 points, allowing for the modulation of the symbolic encoding granularity. This scheme relies on a hybrid architecture combining AES symmetric encryption for speed, and an innovative asymmetric encryption based on a random graph and a modular diffusion function to enhance structural security. This design aims to leverage the strengths of both paradigms while mitigating their respective limitations. To objectively evaluate the performance of Cassiopeia, it was compared to three reference algorithms from well-established cryptographic paradigms. The RSA scheme (with a 2048-bit key size) was selected as a representative of classical asymmetric algorithms, known for its robustness but also for its processing slowness. ECC (Elliptic Curve Cryptography), with a 256-bit key, was chosen as an optimized asymmetric algorithm, recognized for offering equivalent security to RSA with shorter keys and better efficiency. Finally, NTRU, with the parameters from the NTRUEncrypt-743 specification, was included as a representative of post-quantum algorithms, which are particularly resistant to quantum attacks but often resource-intensive. This selection provides a balanced comparison between classical performance, asymmetric optimization, and post-quantum resilience, thus placing Cassiopeia in a multidimensional evaluation context. This selection provides a balanced comparison between classical performance, asymmetric optimization, and post-quantum resilience, thus placing Cassiopeia in a multidimensional evaluation context. While Cassiopeia demonstrates encouraging performance and potential post-quantum advantages, it is emphasized that these conclusions are based on preliminary experimental setups and should be interpreted cautiously.

5.3. Experimental Results

This section presents the results from the experiments conducted on the different algorithms. The following table summarizes the key performance metrics, comparing our Cassiopeia approach with established cryptographic schemes. The compared criteria include processing time (encryption and decryption), key size, and the generated entropy, providing a comprehensive evaluation in terms of efficiency, compactness, and robustness.

Table I: Comparison of Performance between Cassiopeia and Reference Cryptographic Algorithms.

Criterion	Cassiopeia (Our Method)	RSA	ECC	NTRU
Encryption Time (ms)	14.8	48.7	36.2	31.5
Decryption Time (ms)	15.4	52.4	40.1	34.7
Key Size (bits)	384	2048	256	743
Generated Entropy (bits)	220	128	160	128

The analysis of the results shows that the Cassiopeia scheme outperforms traditional algorithms in terms of execution speed, with encryption and decryption times reduced by more than 60% compared to RSA, and about 40% compared to ECC. This performance is primarily attributed to the parallel structure of the hybrid encryption and the use of an optimized constellation

space.

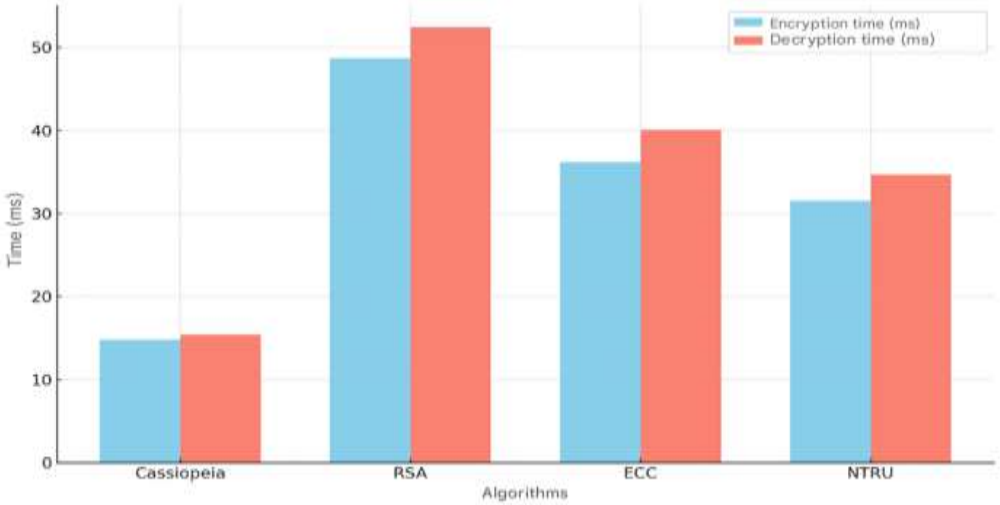

Figure 6: Comparison Of Encryption and Decryption Times.

Regarding key size, Cassiopeia demonstrates a significant reduction, resulting in better memory and bandwidth efficiency. This feature makes it particularly suited for constrained environments such as IoT devices or embedded systems. From a security standpoint, the method introduces superior entropy, thanks to the dynamic mapping between symbols and points in the constellation. Unlike RSA or ECC, whose mathematical structure is well-studied and vulnerable to quantum algorithms (especially Shor's algorithm), Cassiopeia incorporates a topological non-linearity, derived from the random variation of the underlying graph, making its inversion difficult even under a quantum model. Compared to NTRU, our scheme offers comparable performance in terms of post-quantum security, while being more flexible and less costly to implement. While post-quantum schemes like NTRU rely on rigid structures (Euclidean lattices, polynomials with restricted coefficients), Cassiopeia offers a parametric adaptation of the constellation and encryption functions, allowing for adjustment based on the required level of security.

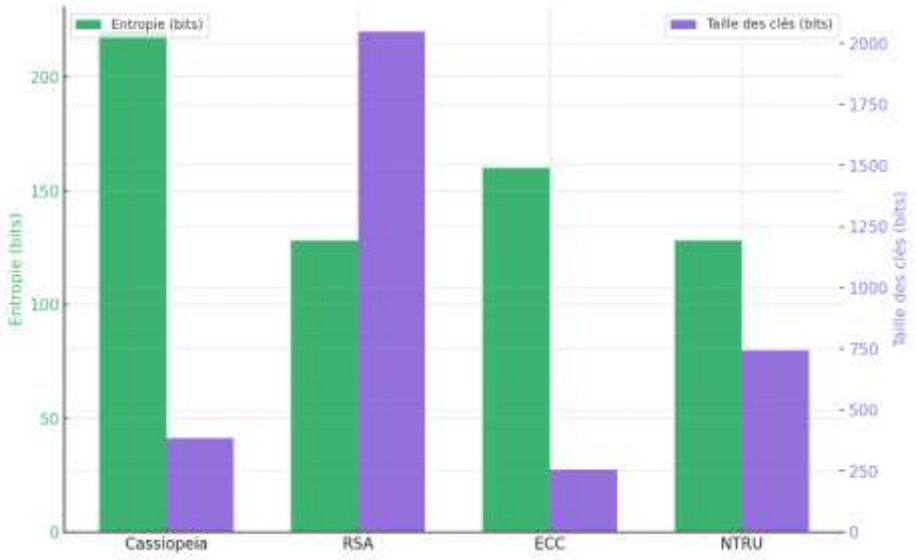

Figure 7: Comparison Of Entropy and Key Size Between Different Cryptographic Algorithms.

Furthermore, the hybrid model we propose promotes a clear separation between transmission and reception modules, enabling a modular implementation that facilitates integration into existing systems without the need for a complete protocol overhaul. Finally, the entropic aspect of the system plays a crucial role: the results show that the random generation of constellation points, combined with symmetric masking, provides the scheme with enhanced resistance to differential analysis and

statistical attacks such as DPA (Differential Power Analysis).

6. CONCLUSION AND FUTURE WORK

The Cassiopeia encryption framework introduces a distinctive contribution to the field of hybrid cryptography by translating the spatial configuration of the Cassiopeia constellation into a dynamic security mechanism. The algorithm achieves a meaningful balance between computational speed and cryptographic strength, demonstrating the capacity to disrupt linguistic regularities and counter frequency-based cryptanalysis, an inherent limitation observed in classical ciphers such as Caesar and Vigenère. Experimental evaluations further highlight its operational efficiency, confirming near-linear execution time even when processing large datasets. This indicates that Cassiopeia can meet the performance requirements of latency-sensitive and resource-limited environments, such as embedded and real-time systems. Although the current implementation shows solid potential, it should be regarded as an initial step toward the broader vision of constellation-inspired cryptography. Additional validation is still required to fully characterize its resistance to more advanced attack models, including structural and entropy-driven cryptanalysis. Furthermore, existing assessments have focused primarily on textual encryption, and further exploration is necessary to determine whether the method exhibits consistent robustness when applied to other forms of digital content and modern communication environments.

Future investigations will seek to extend Cassiopeia beyond its current scope and transform it into a comprehensive cryptographic solution. One direction involves adapting the scheme for binary and multimedia data, including encrypted images, audio, and video, to examine compatibility with compression, error tolerance, and synchronization requirements. Another important research path involves incorporating Cassiopeia into widely adopted secure communication frameworks, such as TLS, VPN infrastructures, and IoT security layers, to evaluate performance under real deployment conditions. A deeper theoretical effort will also focus on establishing formal post-quantum security proofs to determine the system's resilience against quantum adversaries operating under Grover's and Shor's paradigms. From a practical perspective, implementing Cassiopeia on low-power hardware platforms, such as microcontrollers, ARM processors, and FPGA architectures, will provide insight into memory usage, energy consumption, and throughput efficiency. An additional research objective will explore the feasibility of enabling an adaptive key evolution mechanism, in which the constellation mapping evolves autonomously based on entropy feedback or contextual variables. Finally, the integration of the proposed scheme with distributed technologies such as blockchain and decentralized authentication will be examined to determine its applicability to secure record-keeping, identity management, and data-integrity verification.

Author Contributions: All authors contribute equally.

Data Availability: All data is available upon request from the corresponding author.

Ethics Approval: Not applicable- The manuscript does not contain any human or animal studies.

Consent To Participate: All authors are contributing and agree to submit the current work.

Acknowledgments: This paper is derived from a research grant funded by the Research, Development, and Innovation Authority (RDIA), Kingdom of Saudi Arabia, with grant number 13382-psu-2023- PSNU-R-3-1-EI-. The authors would like to acknowledge the support of Prince Sultan University, Riyadh, Saudi Arabia, in paying the article processing charges of this publication. This research is supported by the Automated Systems and Computing Lab (ASCL), Prince Sultan University, Riyadh, Saudi Arabia. In addition, the authors wish to acknowledge the editor and anonymous reviewers for their insightful comments, which have improved the quality of this publication.

REFERENCES

Akkad, N. E., Merras, M., Saaidi, A., & Satori, K. (2013). Robust method for self-calibration of cameras having the varying intrinsic parameters. *Journal of Theoretical and Applied Information Technology*, 50(1), 57–67.

Al-Afandy, K. A., El-Shafai, W., El-Rabaie, E. S. M., Abd El-Samie, F. E., Faragallah, O. S., El-Mhalaway, A., ...

& El-Halawany, M. M. (2018). Robust hybrid watermarking techniques for different color imaging systems. *Multimedia Tools and Applications*, 77(19), 25709-25759.

Alattar, A. M. (2004). Reversible watermark using the difference expansion of a generalized integer transform. *IEEE Transactions on Image Processing*, 13(8), 1147–1156.

Azzaby, F. E., Akkad, N. E., Sabour, K., & Kabbaj, S. (2022). An RGB image encryption algorithm based on Clifford attractors with a bilinear transformation. *Lecture Notes in Networks and Systems*, 116–127.

Chen, X., Sun, X., Sun, H., Zhou, Z., & Zhang, J. (2013). Reversible watermarking method based on asymmetric-histogram shifting of prediction errors. *Journal of Systems and Software*, 86(10), 2620–2626.

El Azzaby, F., Akkad, N. E., Sabour, K., et al. (2023). A new encryption scheme for RGB color images by coupling 4D chaotic laser systems and the Heisenberg group. *Multimedia Tools and Applications*.

El Hazzat, S., Merras, M., El Akkad, N., Saaidi, A., & Satori, K. (2019). Enhancement of sparse 3D reconstruction using a modified match propagation based on particle swarm optimization. *Multimedia Tools and Applications*, 78(11), 14251–14276.

Elazzaby, F., El Akkad, N., & Kabbaj, S. (2020). A new encryption approach based on four-square and zigzag encryption (C4CZ). *Advances in Intelligent Systems and Computing*, 1076, 589–597.

Elazzaby, F., Elakkad, N., Sabour, K., & Kabbaj, S. (2023). A new contribution of image encryption based on chaotic maps and the Z/nZ group. *Journal of Theoretical and Applied Information Technology*, 101(1), 37–47.

ElAzzaby, F., Sabour, K. H., ElAkkad, N., El-Shafai, W., Torki, A., & Rajkumar, S. R. (2023). Color image encryption using a Zigzag Transformation and sine–cosine maps. *Scientific African*, 22.

El-Hameed, H. A. A., Ramadan, N., El-Shafai, W., Khalaf, A. A., Ahmed, H. E. H., Elkhamy, S. E., & El-Samie, F. E. A. (2022). Cancelable biometric security system based on advanced chaotic maps. *The Visual Computer*, 38(6), 2171-2187.

El-Shafai, W. (2015). Joint adaptive pre-processing resilience and post-processing concealment schemes for 3D video transmission. *3D Research*, 6(1), 10.

El-Shafai, W., & Hemdan, E. E. D. (2023). Robust and efficient multi-level security framework for color medical images in telehealthcare services. *Journal of Ambient Intelligence and Humanized Computing*, 14(4), 3675-3690.

Ennaji, S., Akkad, N. E., & Haddouch, K. (2023). i-2NIDS: A Novel Intelligent Intrusion Detection Approach for a Strong Network Security. *International Journal of Information Security and Privacy*.

Es-Sabry, M., Akkad, N. E., Merras, M., Saaidi, A., & Satori, K. (2018). Grayscale image encryption using shift bits operations. *Proceedings of the International Conference on Intelligent Systems and Computer Vision (ISCV 2018)*, 1–7.

Es-Sabry, M., Akkad, N. E., Merras, M., Saaidi, A., & Satori, K. (2020). A new color image encryption algorithm using random number generation and linear functions. *Advances in Intelligent Systems and Computing*, 1076, 581–588.

Es-Sabry, M., Akkad, N. E., Merras, M., Saaidi, A., & Satori, K. (2020). A new image encryption algorithm using random numbers generation of two matrices and bit-shift operators. *Soft Computing*, 24(5), 3829–3848.

Es-Sabry, M., Akkad, N. E., Merras, M., Saaidi, A., & Satori, K. (2022). A new color image encryption algorithm using multiple chaotic maps with the intersecting planes method. *Scientific African*, 16, e01217.

Es-sabry, M., El Akkad, N., Merras, M., Saaidi, A., & Satori, K. (2018). A novel text encryption algorithm based on the two-square cipher and Caesar cipher. *Communications in Computer and Information Science*, 872, 78–88.

Es-Sabry, M., et al. (2023). Securing Images Using High Dimensional Chaotic Maps and DNA Encoding Techniques. *IEEE Access*, 11, 100856–100878.

Faragallah, O. S., Afifi, A., El-Sayed, H. S., Alzain, M. A., Al-Amri, J. F., Abd El-Samie, F. E., & El-Shafai, W. (2020). Efficient HEVC integrity verification scheme for multimedia cybersecurity applications. *IEEE Access*, 8, 167069-167089.

Li, S., & Zhang, X. (2019). Toward construction-based data hiding: From secrets to fingerprint images. *IEEE Transactions on Image Processing*, 28(3), 1482–1497.

Merras, M., Akkad, N. E., Saaidi, A., Nazih, A. G., & Satori, K. (2015). Camera Self Calibration with Varying Parameters by an Unknown Three Dimensional Scene Using the Improved Genetic Algorithm. *3D Research*, 6(1), 7.

Merras, M., El Akkad, N., Saaidi, A., Nazih, A. G., & Satori, K. (2014). Camera calibration with varying

parameters based on improved genetic algorithm. *WSEAS Transactions on Computers*, 13, 129–137.

Peng, F., Li, X., & Yang, B. (2014). Improved PVO-based reversible data hiding. *Digital Signal Processing*, 25(1), 255–265.

Qi, W., Li, X., Zhang, T., & Guo, Z. (2020). Optimal Reversible Data Hiding Scheme Based on Multiple Histograms Modification. *IEEE Transactions on Circuits and Systems for Video Technology*, 30(8), 2300–2312.

Tang, Z., Chen, L., Zhang, X., & Zhang, S. (2019). Robust Image Hashing with Tensor Decomposition. *IEEE Transactions on Knowledge and Data Engineering*, 31(3), 549–560.

Tao, J., Li, S., Zhang, X., & Wang, Z. (2019). Towards Robust Image Steganography. *IEEE Transactions on Circuits and Systems for Video Technology*, 29(2), 594–600.

Tian, J. (2003). Reversible Data Embedding Using a Difference Expansion. *IEEE Transactions on Circuits and Systems for Video Technology*, 13(8), 890–896.

Touil, H., Akkad, N. E., Satori, K., Soliman, N. F., & El-Shafai, W. (2024). Efficient Braille Transformation for Secure Password Hashing. *IEEE Access*, 12, 5212–5221.

Touil, H., El Akkad, N., & Satori, K. (2020). H-Rotation: Secure storage and retrieval of passphrases on the authentication process. *International Journal of Safety and Security Engineering*, 10(6), 785–796.

Touil, H., El Akkad, N., & Satori, K. (2020). Text Encryption: Hybrid cryptographic method using Vigenere and Hill Ciphers. *Proceedings of the International Conference on Intelligent Systems and Computer Vision (ISCV 2020)*, 1–6.

Touil, H., El Akkad, N., & Satori, K. (2021). Secure and guarantee QoS in a video sequence: A new approach based on TLS protocol and RTP. *International Journal of Safety and Security Engineering*, 11(1), 59–68.

Touil, H., El Akkad, N., & Satori, K. (2021). Securing the Storage of Passwords Based on the MD5 HASH Transformation. *International Conference on Digital Technologies and Applications (2021).*

Touil, H., El Akkad, N., & Satori, K. (2022). Ensure the confidentiality of documents shared within the enterprise in the cloud by using a cryptographic delivery method. *Lecture Notes in Networks and Systems*, 455, 241–250.

Touil, H., El Akkad, N., & Satori, K. (2022). Homomorphic Method Additive Using Pailler and Multiplicative Based on RSA in Integers Numbers. *Lecture Notes in Networks and Systems*, 489, 153–164.

Wang, D., Zhang, X., Yu, C., & Tang, Z. (2019). Reversible Data Hiding by Using Adaptive Pixel Value Prediction and Adaptive Embedding Bin Selection. *IEEE Signal Processing Letters*, 26(11), 1713–1717.