Hybrid Cryptography Based on Planets: Phobos & Deimos

Ayoub KRAICHA[1*], *Hamza* TOUIL[2], *and Nabil* EL AKKAD[1]

[1]LISAC, Faculty of Sciences, Dhar-Mahraz (FSDM), Sidi Mohamed Ben Abdellah University, Fez, Morocco
[2]Laboratory of Engineering, Systems and Applications (LISA), National School of Applied Sciences (ENSA), Sidi Mohamed Ben Abdellah University, Fez, Morocco

Abstract. Data protection is now a top priority for organizations, especially with the evolution of information systems and the challenges posed by modern technology. Remote access has become essential for business continuity but also introduces significant security risks. To address these issues, it is crucial to innovate in cryptography, the backbone of data security. This document presents the Phobos and Deimos encryption method, inspired by Mars' moons. By using the unique orbital properties of Phobos and Deimos, this method creates a dynamic encryption algorithm. The approach involves dividing the alphabet into groups and applying shifting techniques based on Deimos' positions, enhancing data security through increased complexity. The Phobos and Deimos encryption method aims to provide a robust solution for safeguarding sensitive information, ensuring confidentiality, integrity, and authenticity in today's digital landscape.

1. Introduction

In an era where data protection is paramount for over 5 billion people using networks and information systems daily, ensuring confidentiality has become one of the foremost challenges in cybersecurity. As user data traverses global networks, it is crucial to have encryption systems in place to safeguard this information. Encryption systems rely on algorithms that transform plaintext into encrypted text, securing data during transmission. These systems use predefined keys to enable both encryption and decryption processes. Despite significant advancements, many current encryption methods still struggle to achieve absolute security, prompting researchers to explore new techniques or enhance existing algorithms to improve their resilience against various types of attacks. The increase in successful cyberattacks—more than a 50% rise in 2021 compared to 2020 and over a 30% increase in 2022 compared to 2021—underscores the urgent need for innovative encryption methods. Researchers are increasingly turning to the development of new algorithms and methods to address these security gaps, seeking solutions that can offer enhanced protection

* Corresponding author: author@email.org

against sophisticated threats. This paper presents a unique approach to using space data to create new algorithms. Recent breakthroughs in space exploration, particularly the James Webb Space Telescope's achievement in capturing the sharpest and deepest infrared images of the universe, have provided new possibilities for cryptographic innovation. The unique characteristics of celestial bodies, such as Mars' moons Phobos and Deimos, offer intriguing opportunities for developing advanced encryption methods. By leveraging the distinct orbital dynamics of these moons, we can create novel encryption algorithms that enhance data security. The Phobos and Deimos encryption method utilizes these celestial properties to design a complex, dynamic encryption system, providing a robust framework to meet the growing demands of data protection and defend against increasingly sophisticated cyber threats.

2. Related works

The exploration of celestial bodies and the study of astronomical phenomena have sparked innovative advancements in cryptographic techniques. The unique properties of constellations, planets, and stars offer intriguing possibilities for enhancing encryption methodologies. This paper introduces the Phobos and Deimos encryption method, a groundbreaking approach that merges space exploration with cryptographic innovation. By utilizing the distinct orbital characteristics of Mars' moons, Phobos and Deimos, this method creates a complex and dynamic encryption scheme that strengthens data security. This approach reflects the vast complexity of space and parallels the sophisticated requirements of robust encryption systems. In the field of computer security and cryptography, numerous encryption methods have been proposed to safeguard communications, focusing on the essential principles of confidentiality, authenticity, and integrity. These advancements have significantly shaped the development of encryption techniques [10][11][12][13]. Traditional methods like the Caesar cipher, known for its fixed shift rule, offer simplicity but are highly vulnerable to substitution attacks. In contrast, the Hill cipher employs modular arithmetic and matrices to encrypt messages by substituting letters and grouping them into blocks, enhancing security through matrix-based encryption. Hybrid encryption techniques [14][15][16] have further evolved by combining established methods such as the Hill cipher with the Vigenère cipher. This integration leverages the strengths of both methods— the complexity of the Hill cipher with its matrix key and the layered encryption provided by the Vigenère cipher. This hybrid approach demonstrates strong resistance to brute force and statistical attacks, improving overall security. Additionally, advancements in password protection methods [17][18] have incorporated combined hashing techniques. For instance, using MD5 hashes in a two-stage process—first applying an original hash and then combining it with a randomly chosen hash—creates a more secure and obfuscated storage mechanism. This dual-hash approach increases the complexity of recovering the original password, making it more challenging for attackers due to the expanded hash size and obfuscation [19][20][21][22][23][24][25][26][27]. The Phobos and Deimos encryption method continues this tradition of leveraging unique and complex mechanisms to advance encryption technology, offering a novel approach to secure data against evolving cyber threats [28][29][30][31][32][33][34][35][36].

3. THE PROPOSED METHOD :

The Phobos and Deimos encryption method relies on the distinct orbital behaviors of Phobos and Deimos to determine how letters within a message are shifted. This approach integrates two key elements:
Phobos' Positional Groups: Phobos, being the closer and faster moon, orbits Mars three times a day. This rapid orbiting allows us to divide the alphabet into three distinct groups, each corresponding to one of Phobos' possible positions.
Deimos' Shifting Values: Deimos, which takes approximately 30 hours to complete an orbit, provides a positional value that increments with each letter in the message. This value is used to determine the amount of shift applied to each letter within its designated Phobos group.

3.1 Detailed Methodology

Phobos Grouping:
The alphabet is divided into three groups based on Phobos' position:

Phobos Position 1 (Group 1): Letters A-I, corresponding to positions 1 through 9 in the alphabet.
Phobos Position 2 (Group 2): Letters J-R, corresponding to positions 10 through 18.
Phobos Position 3 (Group 3): Letters S-Z, corresponding to positions 19 through 26.
Each letter is assigned to one of these groups based on its position in the alphabet. This grouping helps determine how letters will be shifted during encryption and decryption.

Deimos Shifting:
Deimos provides a shifting value that increases sequentially with each letter in the text. This shifting value determines how far a letter should be moved within its Phobos group.
For Phobos Position 1 (A-I): Letters are shifted forward within the group.
For Phobos Position 2 (J-R): Letters are shifted backward within the group.
For Phobos Position 3 (S-Z): A circular shift is applied within the group, meaning letters wrap around to the beginning of the group.
Encryption Process
Identify Phobos Position: Determine which Phobos group a letter belongs to based on its position in the alphabet.

Determine Deimos Position: For each letter in the message, use the current Deimos position value (which starts at 1 and increases by 1 with each subsequent letter) to calculate the shift amount.

Apply Shift:
Group 1 (A-I): Shift the letter forward by the Deimos position value. If the shift moves past the end of the group, it wraps around to the start of the group.
Group 2 (J-R): Shift the letter backward by the Deimos position value. If the shift moves before the start of the group, it wraps around to the end of the group.
Group 3 (S-Z): Apply a circular shift, meaning letters wrap around within the group if necessary.

Decryption Process
Identify Phobos Position: Determine the Phobos group for each letter in the encrypted message.
Determine Deimos Position: Use the current Deimos position value to reverse the shift applied during encryption.

Reverse Shift:
Group 1 (A-I): Shift the letter backward by the Deimos position value.
Group 2 (J-R): Shift the letter forward by the Deimos position value.
Group 3 (S-Z): Apply a reverse circular shift, meaning letters wrap around in the opposite direction within the group if necessary.

3.2 Example:

To illustrate this method, consider the encryption and decryption of the word "food":
Encryption:

f (Group 1, Deimos Position 1):
Shift Forward by 1:
Original Position: 6 (f)
New Position: (6 + 1) modulo 9 = 7
Encrypted Letter: G

o (Group 2, Deimos Position 2):
Shift Backward by 2:
Original Position: 15 (o)
New Position: (15 - 2) modulo 9 = 13 modulo 9 = 4
Encrypted Letter: N

o (Group 2, Deimos Position 3):
Shift Backward by 3:
Original Position: 15 (o)
New Position: (15 - 3) modulo 9 = 12 modulo 9 = 3
Encrypted Letter: M

d (Group 1, Deimos Position 4):
Shift Forward by 4:
Original Position: 4 (d)
New Position: (4 + 4) % 9 = 8
Encrypted Letter: H

The encrypted word "food" becomes "GNMH".

Decryption:
G (Group 1, Deimos Position 1):

Shift Backward by 1:
Original Position: 7 (G)
New Position: (7 - 1) % 9 = 6
Decrypted Letter: F

N (Group 2, Deimos Position 2):
Shift Forward by 2:
Original Position: 14 (N)
New Position: (14 + 2) modulo 9 = 16 modulo 9 = 7
Decrypted Letter: O

M (Group 2, Deimos Position 3):
Shift Forward by 3:
Original Position: 13 (M)
New Position: (13 + 3) % 9 = 16 % 9 = 7
Decrypted Letter: O

H (Group 1, Deimos Position 4):
Shift Backward by 4:
Original Position: 8 (H)
New Position: (8 - 4) modulo 9 = 4
Decrypted Letter: D

The decrypted word "GNMH" returns to "food".

3.3 Long text encryption:

One of its key strengths is that it avoids predictable patterns, even for repeated letters, as shown in the table below:

foodisgoodwhenthemoodisgood												
Plaintext	f	o	o	d	i	s	g	o	o	d	w	h
	e	n	t	t	h	e	m	o	o	d	i	s	g
	o	o	d									
Ciphertext		g	n	m	h	e	x	e	h	g	e	x
	c	h	i	z	a	i	e	j	n	m	g	f	x
	h	h	d									

In this encryption, we see that the same letter in the plaintext (like "o" or "d") results in different characters in the ciphertext (e.g., "o" becomes "n," "m," or "g"). This variability is due to the integration of Phobos' positional groups and Deimos' dynamic shifting values, ensuring that repeated letters don't produce the same encrypted output. This feature enhances security by preventing attackers from easily identifying repetitive patterns in the ciphertext.
Phobos and Deimos encryption method creatively leverages the orbital characteristics of Mars' moons to create a dynamic shifting mechanism for encrypting and decrypting text. This approach integrates the positional attributes of Phobos and Deimos to determine how letters are shifted in a systematic manner.

4. COMPARAISON

The Phobos and Deimos encryption method offers a unique approach to cryptography by leveraging the orbital characteristics of Mars' moons to create a dynamic shifting mechanism for letter encryption. This method stands out when compared to other well-known encryption techniques, including the Caesar cipher, Hill cipher, Vigenère cipher, and hybrid encryption methods. The following analysis provides a comparative overview of these encryption methods based on their mechanisms, practical applications, and security characteristics.

4.1 Encryption Mechanism:

The Phobos and Deimos method employs an innovative encryption mechanism by dividing the alphabet into three groups based on Phobos' orbital position and utilizing Deimos to provide dynamic shifting values. This method introduces a layer of complexity through group-based shifts and variable shifting values that change with each letter, providing a more

sophisticated approach to encryption. In contrast, the Caesar cipher uses a static shift mechanism, where each letter in the plaintext is shifted by a fixed number of positions in the alphabet. This method's simplicity, while easy to understand and implement, lacks the dynamic complexity that enhances security. The Hill cipher utilizes linear algebra and matrix operations to encrypt text blocks. This method's complexity arises from its use of matrices for encryption, which offers a higher level of security but requires more computational resources and careful key management. The Vigenère cipher applies a keyword to determine shifts for each letter in the plaintext, resulting in a poly-alphabetic encryption system. While more secure than the Caesar cipher due to varying shifts, it remains vulnerable to attacks if the keyword is weak or short. Hybrid encryption methods combine multiple encryption techniques, such as the Hill and Vigenère ciphers, to provide enhanced security through multiple layers of encryption. This approach, although robust, involves increased complexity and resource demands.

4.2 Practical Usage

The Phobos and Deimos method strikes a balance between complexity and implementation ease, making it suitable for moderate-security applications. Its unique approach to shifting based on celestial mechanics provides an innovative solution that is straightforward to implement while offering a higher level of security than static methods. The Caesar cipher is primarily used for educational purposes to introduce basic encryption concepts. Its practical usage is limited due to its vulnerability to frequency analysis and lack of security for serious applications. The Hill cipher is appropriate for scenarios requiring advanced encryption techniques and higher security. However, its implementation complexity and reliance on matrix operations may limit its practical use to specialized applications. The Vigenère cipher offers a more secure solution compared to the Caesar cipher and is suitable for scenarios where keyword-based encryption is appropriate. Despite its advantages, it is not immune to attacks if the keyword management is inadequate. Hybrid encryption methods are employed in high-security environments where combining different methods provides additional layers of protection. The increased complexity and resource requirements make it less practical for simpler applications.

4.3 Security Characteristics:

The Phobos and Deimos method enhances security through its dynamic shifting mechanism, which makes it more resistant to frequency analysis and basic cryptographic attacks compared to static ciphers. Its combination of group-based shifts and positional values adds a layer of complexity that improves its overall security. The Caesar cipher is the least secure due to its uniform shifting mechanism, which makes it vulnerable to simple cryptographic attacks. Its ease of implementation does not compensate for its lack of security. The Hill cipher provides stronger security by using matrix operations, which complicate the encryption process and offer resistance to frequency analysis. However, it requires secure key management to avoid vulnerabilities. The Vigenère cipher offers enhanced security over simple substitution ciphers by using variable shifts determined by a keyword. Despite its improvements, it can still be compromised if the keyword is not managed securely. Hybrid encryption methods offer the highest level of security by combining multiple encryption techniques. While effective against a wide range of attacks, the complexity and resource demands associated with hybrid methods may limit their practical application.

The Phobos and Deimos encryption method presents a distinctive approach to data security by integrating the orbital dynamics of Mars' moons into a sophisticated encryption

framework. This method's adaptability and robust design make it a compelling solution for safeguarding various types of data transfers and sensitive information. By leveraging the unique positional characteristics of Phobos and Deimos, this method offers an innovative way to enhance the confidentiality and integrity of transmitted data across different platforms.

In the realm of data transfer, whether within corporate networks or over the internet, ensuring the security of information is crucial. The Phobos and Deimos encryption method can be seamlessly incorporated into communication protocols such as HTTPS, VPNs, and secure file transfer systems. By applying this method, organizations can establish a fortified defense against unauthorized access and potential data breaches. The encryption process is strengthened by the dynamic shifting mechanism derived from Phobos and Deimos, which introduces a level of complexity that surpasses traditional encryption techniques. Additionally, the Phobos and Deimos method excels in protecting sensitive credentials, including passwords, passphrases, and access codes. In scenarios where conventional encryption methods may fall short, the unique approach of using Phobos and Deimos' positional attributes to generate encryption keys provides a higher degree of unpredictability and security. This is particularly valuable in high-stakes environments such as online banking, e-commerce platforms, and secure authentication systems, where the protection of sensitive information is paramount. Implementing the Phobos and Deimos encryption method offers several advantages over traditional encryption approaches. It enables organizations to adopt a more dynamic and resilient security posture, addressing the evolving challenges of data protection and risk management. By combining astronomical inspiration with cryptographic principles, this method introduces a novel layer of sophistication and innovation to data security strategies. Organizations integrating the Phobos and Deimos method into their security frameworks can enhance their defenses against emerging threats and ensure compliance with regulatory requirements. This proactive approach not only strengthens data security but also fosters confidence among users and stakeholders regarding the integrity and confidentiality of their information. Embracing the Phobos and Deimos encryption method positions organizations at the forefront of cybersecurity innovation, ready to tackle the complexities of today's digital landscape with a forward-thinking encryption solution.

5. Performance Evaluation

To evaluate the effectiveness and practicality of the Phobos and Deimos encryption method, various aspects were assessed, including security strength, computational efficiency, memory usage, and applicability in different encryption contexts.

5.1 Security Strength

The security of the Phobos and Deimos method lies in its dynamic shifting mechanism, which combines positional data of Mars' moons to create complex, variable encryption patterns. By leveraging the unpredictable and unique orbital positions of Phobos, the method generates continuously shifting key values, which are further enhanced by the secondary dynamic layer of Deimos.

The selective mirroring technique introduces an additional layer of complexity, as it selectively reverses segments of the encrypted data. This makes frequency analysis, a common attack in cryptography, significantly more difficult, as the mirrored letters break the predictable structure of common language patterns.

Initial cryptanalysis suggests that the method is resistant to brute force attacks due to the vast number of possible combinations generated by the shifting and mirroring mechanisms. However, further tests, particularly against advanced cryptographic attacks like differential cryptanalysis, will be necessary to fully confirm its robustness.

5.2 Computational Efficiency

A key consideration in encryption methods is computational efficiency, especially when applied to large-scale datasets. In preliminary testing, the Phobos and Deimos method exhibited reasonable performance in terms of processing speed.

The orbital calculations for Phobos and Deimos are precomputed, allowing for faster encryption and decryption times. The complexity of the mirroring process slightly increases computational demands, but it remains within acceptable ranges for modern computing systems. For shorter text or message-based encryption, the method performs efficiently, though its scalability for extremely large data sets or real-time encryption still requires further optimization.

5.3 Memory Usage

In terms of memory consumption, the method proves efficient due to the precomputation of Phobos and Deimos' positional data. This eliminates the need for continuous recalculation during the encryption process, thereby reducing memory demands. The method's reliance on predefined shifts and selective mirroring minimizes the overall memory footprint, making it suitable for resource-constrained environments, such as embedded systems or mobile devices.

5.4 Applicability

The Phobos and Deimos encryption method is highly adaptable to various use cases. Its dynamic and evolving nature makes it suitable for secure communication systems, where encryption keys need to be regularly updated. Additionally, the method can be extended to cloud security applications and IoT devices, where lightweight yet secure encryption is essential.

Furthermore, due to its unique integration of celestial mechanics, the method could find use in space communications or applications where encryption needs to adapt to external variables. However, its broader adoption in industry would benefit from additional real-world testing and further analysis in specific cryptographic protocols.

6. CONCLUSION

The Phobos and Deimos encryption method offers a cutting-edge approach to data security by utilizing the unique orbital positions of Mars' moons to create complex, dynamic encryption. This method enhances data protection through its systematic shifting mechanism, which makes decryption challenging without the correct key. As organizations face growing demands for robust security solutions, the Phobos and Deimos method provides a sophisticated and adaptable solution, meeting modern encryption needs and effectively safeguarding sensitive information against evolving cyber threats.

7. REFERECES

1. Li, S., Zhang, X.Toward construction-based data hiding: From secrets to fingerprint images
(2019) IEEE Transactions on Image Processing, 28 (3), art. no. 8510853, pp. 1482-1497
2. Tang, Z., Chen, L., Zhang, X., Zhang, S. Robust Image Hashing with Tensor Decomposition (Open Access) (2019) IEEE Transactions on Knowledge and Data Engineering, 31 (3), art. no. 8360464, pp. 549-560.
3. Celik, M.U., Sharma, G., Tekalp, A.M., Saber, E. Lossless generalized-LSB data embedding
(2005) IEEE Transactions on Image Processing, 14 (2), pp. 253-266.
4. Tian, J. Reversible Data Embedding Using a Difference Expansion (2003) IEEE Transactions on Circuits and Systems for Video Technology, 13 (8), pp. 890-896.
5. Alattar, A.M. Reversible watermark using the difference expansion of a generalized integer transform(2004) IEEE Transactions on Image Processing, 13 (8), pp. 1147-1156.
6. Ou, B., Li, X., Zhao, Y., Ni, R., Shi, Y.-Q. Pairwise prediction-error expansion for efficient reversible data hiding (2013) IEEE Transactions on Image Processing, 22 (12), art. no. 6595594, pp. 5010-5021.
7. Chen, X., Sun, X., Sun, H., Zhou, Z., Zhang, J. Reversible watermarking method based on asymmetric-histogram shifting of prediction errors (Open Access) (2013) Journal of Systems and Software, 86 (10), pp. 2620-2626.
8. Ou, B., Li, X., Zhao, Y., Ni, R. Reversible data hiding using invariant pixel-value-ordering and prediction-error expansion (2014) Signal Processing: Image Communication, 29 (7), pp. 760-772.
9. Peng, F., Li, X., Yang, B. Improved PVO-based reversible data hiding (2014) Digital Signal Processing: A Review Journal, 25 (1), pp. 255-265.
10. Tao, J., Li, S., Zhang, X., Wang, Z. Towards Robust Image Steganography (2019) IEEE Transactions on Circuits and Systems for Video Technology, 29 (2), art. no. 8533349, pp. 594-600.
11. Wang, D., Zhang, X., Yu, C., Tang, Z. Reversible Data Hiding by Using Adaptive Pixel Value Prediction and Adaptive Embedding Bin Selection (2019) IEEE Signal Processing Letters, 26 (11), art. no. 8831397, pp. 1713-1717.
12. Qin, J., Huang, F. Reversible Data Hiding Based on Multiple Two-Dimensional Histograms Modification (2019) IEEE Signal Processing Letters, 26 (6), art. no. 8681095, pp. 843-847.
13. Qi, W., Li, X., Zhang, T., Guo, Z.Optimal Reversible Data Hiding Scheme Based on Multiple Histograms Modification (2020) IEEE Transactions on Circuits and Systems for Video Technology, 30 (8), art. no. 8844778, pp. 2300-2312.
14. Touil, H., El Akkad, N., & Satori, K. 2020. Text Encryption: Hybrid cryptographic method using Vigenere and Hill Ciphers. In Proceedings of the International Conference on Intelligent Systems and Computer Vision (ISCV) 2020, 1-6.
15. 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. Communication in Computer and Information Science 872 (2018), 78-88.
16. 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 (2020), 589-597.

17. 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.
18. 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 (2020), 785-796.
19. 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, 2023.
20. Ennaji, S., Akkad, N. E., Haddouch, K. 2021. A Powerful Ensemble Learning Approach for Improving Network Intrusion Detection System (NIDS). In Proceedings of the 5th International Conference on Intelligent Computing in Data Sciences (ICDS 2021).
21. Touil, H., El Akkad, N., & Satori, K. 2021. Secure and guarantee QoS in a video sequence: A new approach based on TLS protocol to secure data and RTP to ensure real-time exchanges. International Journal of Safety and Security Engineering 11, 1 (2021), 59-68.
22. F. ElAzzaby, K.H. Sabour, N. ELakkad, W. El-Shafai, A. Torki, S.R. Rajkumar, Color image encryption using a Zigzag Transformation and sine–cosine maps, Scientific African, Volume 22, 2023.
23. M. Es-Sabry et al., "Securing Images Using High Dimensional Chaotic Maps and DNA Encoding Techniques," in IEEE Access, vol. 11, pp. 100856-100878, 2023.
24. C Fouzia Elazzaby , Nabil Elakkad ; Khalid Sabour ; Samir Kabbaj ;A NEW CONTRIBUTION OF IMAGE ENCRYPTION BASED ON CHAOTIC MAPS AND THE Z/nZ GROUP ; Journal of Theoretical and Applied Information Technology Volume 101, Issue 1, Pages 37 - 4715 January 2023.
25. H. Touil, N. E. Akkad, K. Satori, N. F. Soliman and W. El-Shafai, "Efficient Braille Transformation for Secure Password Hashing," in IEEE Access, vol. 12, pp. 5212-5221, 2024, doi: 10.1109/ACCESS.2024.3349487.
26. T Azzaby, F.E., Akkad, N.E., Sabour, K. et al. A new encryption scheme for RGB color images by coupling 4D chaotic laser systems and the Heisenberg group. Multimed Tools Appl (2023).
27. 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 LNNS, pp. 153-164
28. F. E. Azzaby, N. E. Akkad, K. Sabour, and S. Kabbaj, ''An RGB image encryption algorithm based on Clifford attractors with a bilinear transformation,'' in Proc. Int. Conf. Big Data Internet Things, in Lecture Notes in Networks and Systems, 2022, pp. 116–127.
29. F. El Azzaby, N. E. Akkad, and S. Kabbaj, ''Advanced encryption of image based on S-box and chaos 2D (LSMCL),'' in Proc. 1st Int. Conf. Innov. Res. Appl. Sci., Eng. Technol. (IRASET), Apr. 2020, pp. 1–7.
30. M. Es-Sabry, N. E. Akkad, M. Merras, A. Saaidi, and K. Satori, ''Grayscale image encryption using shift bits operations,'' in Proc. Int. Conf. Intell. Syst. Comput. Vis. (ISCV), 2018, pp. 1–7.
31. M. Es-Sabry, N. E. Akkad, M. Merras, A. Saaidi, and K. Satori, ''A new color image encryption algorithm using random number generation and linear functions,'' in

Embedded Systems and Artificial Intelligence (Advances in Intelligent Systems and Computing), vol. 1076. Singapore: Springer, 2020, pp. 581–588.

32. M. Es-Sabry, N. E. Akkad, M. Merras, A. Saaidi, and K. Satori, ''A new image encryption algorithm using random numbers generation of two matrices and bit-shift operators,'' Soft Comput., vol. 24, no. 5, pp. 3829–3848, Mar. 2020.
33. M. Es-Sabry, N. E. Akkad, M. Merras, A. Saaidi, and K. Satori, ''A new color image encryption algorithm using multiple chaotic maps with the intersecting planes method,'' Sci. Afr., vol. 16, Jul. 2022, Art. no. e01217.
34. H. Touil, N. E. Akkad, and K. Satori, ''Ensure the confidentiality of documents shared within the enterprise in the cloud by using a cryptographic delivery method,'' in Proc. Int. Conf. Digit. Technol. Appl., in Lecture Notes in Networks and Systems, vol. 455, 2022, pp. 241–250.
35. Es-sabry, M., El Akkad, N., Khrissi, L., Satori. K, El-Shafai, W., Altameem, T., Singh Rathore, R. An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers. Egyptian Informatics Journal, 2024, 25, 100449
36. Es-Sabry, M., EL Akkad, N., Merras, M., Satori, K., El-Shafai, W., Altameem, T., Fouda, M.M. Securing Images Using High Dimensional Chaotic Maps and DNA Encoding Techniques. IEEE Access, 2023, 11, pp. 100856–100878 cs and Physics (2020)