

Paper Type: Original Article

Multi-Criteria Security and Attack Resistance Analysis of Matrix-Based Encryption Scheme

Suhaib Badran ¹  and Asmaa Alqassab ^{1,*} 

¹ Department of Computer Science, College of Education for Pure Science, University of Mosul, Mosul, Iraq;
Emails: suhaib.24esp5@student.uomosul.edu.iq; asmaa_mow@uomosul.edu.iq.

Received: 05 Jan 2026

Revised: 12 Apr 2026

Accepted: 29 Jul 2026

Published: 23 Sep 2026

Abstract

In this paper, we analyze the security of a novel matrix-based encryption algorithm by systematically evaluating its resistance to five major types of attacks: brute-force attacks, statistical analysis, differential cryptanalysis, linear cryptanalysis, and chosen-ciphertext attack (CCA) oracle tests. The algorithm is based on text-derived keys, reversible matrix transformations, and bit-level operations to provide cryptographic security. To evaluate the security features, we use seven different metrics: entropy visualization, ECB Detector, Bit Balance, Runs Test, Avalanche Effect, Compression Test, and LZ Complexity. We evaluate each metric before and after applying each type of attack and provide a comparison to understand the impact of different types of attacks on the ciphertext. In experimental tests, we find that the algorithm shows an average resistance score of 60.0% for all types of attack with statistical randomness (high entropy) and diffusion properties (strong avalanche effect). The metric analysis shows that although the algorithm is compromised in key space size and deterministic key derivation, it exhibits good statistical properties that are resistant to pattern-based and frequency-analysis attacks. The results show the effectiveness of the seven-metric framework in providing a multi-dimensional security assessment and also point to areas for improvement in key management and non-linear component integration.

Keywords: Matrix Cryptography; Cryptanalysis; Security Metrics; Cipher Robustness; Linear Cryptanalysis.

1 | Introduction

Cryptographic attacks are a major threat to information security as hackers continue to develop sophisticated methods to hack into encryption systems. Understanding the way encryption algorithms respond to different attack methods is essential to understanding their security status and vulnerabilities. In this paper, we have conducted a comprehensive security analysis of a matrix-based encryption algorithm and characterized its resistance to five main attack types by analyzing the impact of these attacks on seven security metrics. Cryptographic attacks can be described in general in terms of their method and assumptions about the attacker's capabilities. Brute force attacks are the most straightforward, as they try each one systematically. The effectiveness of brute force attacks depends on the size of the key space and on the number of resources available to the attacker. Statistical analysis attacks exploit patterns and regularities in the ciphertext - e.g., frequency distributions of characters or repeating patterns - to extract information



Corresponding Author: asmaa_mow@uomosul.edu.iq



<https://doi.org/10.61356/j.nois.2026.11664>



Licensee **Neutrosophic Optimization and Intelligent systems**. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

about the plaintext or key. They are particularly effective in the case of failing to eliminate statistical properties present in the input. Differential cryptanalysis is a powerful technique for analyzing the impact of small changes in the plaintext on the ciphertext. It can find patterns in the plaintext and the corresponding ciphertexts that can shed light on the key of the cipher or the ciphertext itself. Linear cryptanalysis searches for linear approximations between plaintext bits, ciphertext bits, and key bits. If we find these approximations biased enough, they can be exploited to recover key information with fewer plaintext-ciphertext pairs compared to brute-force attacks. Finally, chosen-ciphertext attack (CCA) oracle tests exploit information leakage by sending a message or timing variation when the attacker submits modified ciphertexts to the system and is able to detect it [1, 2].

We use seven security metrics that analyze different aspects of cryptographic strength to analyze the security of an algorithm, and this gives us a multi-dimensional picture of how different attacks affect different aspects of security. Based on the metric values before and after each attack type, we can measure the encryption algorithm's resistance and also determine which aspects of security are most affected by different attack methods. For example, correlation coefficient analysis measures how closely ciphertexts are, and it also assesses whether the encryption algorithm is able to reduce statistical attacks due to the low correlation between neighboring pixels. Similarly, histogram analysis determines the distribution of pixel values to ensure uniformity of the values and to avoid frequency analysis. Information entropy measures the unpredictability and randomness of ciphertexts [3].

The rest of this paper is organized as follows. Section 2 summarizes other results for attack resistance evaluation and security metrics. Section 3 gives a brief overview of the encryption algorithm. The detailed analysis of each type of attack is presented in Section 4, and its impact on the seven-security metrics is discussed. Section 5 presents the results and their potential implications. Section 6 concludes and explores future development plans.

The main contributions of this study are as follows. First, we propose a seven-metric evaluation framework (entropy visualization, ECB detection, bit balance, runs test, avalanche effect, compression test, and LZ complexity) that provides a multi-dimensional assessment of ciphertext security, extending beyond the three-to-four metric approaches commonly used in prior work. Second, we systematically evaluate the resistance of a matrix-based text encryption algorithm against five distinct attack categories—brute force, statistical analysis, differential cryptanalysis, linear cryptanalysis, and CCA oracle tests—and quantify the before-and-after impact of each attack on all seven metrics. Third, we identify and characterize a concrete security trade-off in the algorithm: strong statistical randomness and diffusion properties (high entropy and avalanche effect) coexist with a critically small key space and deterministic key derivation, offering practical guidance on where the design should be strengthened. Finally, we compare our results quantitatively against prior matrix-based and text-based encryption security evaluations, showing an improvement in average resistance score and a more detailed attack-by-attack breakdown than previously reported.

2 | Related Works

Previous studies have extensively explored different types of cryptanalysis techniques, such as chosen plaintext attacks, known plaintext attacks, and brute force methods, in order to test the robustness of encryption algorithms [4]. For example, researchers have used differential cryptanalysis to evaluate how sensitive an algorithm is to small changes in the input and have often used NPCR and UACI to measure resistance [5]. Other common security analysis metrics include histogram analysis, entropy, contrast, correlation, energy, and homogeneity of cipher images to compare them with plaintext images for encryption. Several studies have also shown that correlation coefficients across different directions (horizontal, vertical, diagonal) are important to assess whether a cryptosystem is strong against statistical attacks [6, 7]. Such metrics together are very powerful in order to determine the strength of an algorithm against statistical attacks [8]. The security of encryption algorithms through attack evaluation has been widely studied in cryptography literature. Biham and Shamir [9] developed differential cryptanalysis and

showed it is effective against DES, and provided a framework to analyze how input differences propagate through cipher operations. Matsui [10] developed linear cryptanalysis and demonstrated that linear approximations can be exploited to recover keys with fewer plaintext-ciphertext pairs than brute-force attacks. These works underlined the need for an attack evaluation in cryptography design. We have recently seen a growing interest in statistical attack resistance, especially in image encryption, where histogram analysis, correlation analysis, entropy analysis, and robustness analysis are applied to measure the resilience of image encryption algorithms to pattern-based attacks [2, 11]. For example, the correlation coefficients of plain images are close to one, while those of ciphers are close to zero, which means that attackers cannot gain useful correlation information to compromise the cryptosystem [3, 12]. Recent work has focused on developing a comprehensive security metric for evaluating encryption algorithms. Wang et al. [13] proposed a multi-metric approach to assess cryptographic strength, including entropy analysis, avalanche effect measurement, and statistical randomness tests. By analyzing a number of block ciphers in detail, it was shown that no single metric is sufficient for a complete security assessment and that a multi-dimensional approach is necessary. However, their work was mainly focused on already known algorithms, and they did not provide detailed before- and after-attack analysis. In contrast, we study the impact of five different types of attacks on the encryption algorithm in a specific manner by measuring changes in seven security metrics, which provide more detailed information about the security weaknesses and strengths of the algorithm. This method allows us to measure the attack resistance of an algorithm at a more detailed level by quantifying the security of the algorithm against different types of attacks and providing quantitative evidence that the security of the algorithm is degraded for specific adversarial scenarios [14]. Such fine-grained analysis is of high importance in order to identify the subtle weaknesses that are not evident from the general level of security metrics alone, especially when cryptanalysis techniques such as machine learning are used in cryptography [15]. Tolba [16] compared the attack resistance of different types of encryption algorithms using statistical measures such as entropy, bit balance, and compression ratio and found that algorithms with good diffusion properties (avalanche effect) proved to be more resistant to statistical and differential attacks. But their analysis was restricted to three metrics and did not include linear cryptanalysis or CCA oracle tests. Our work is a further extension of this study using seven metrics and measuring five attack categories. Chen et al. [17] evaluated the security of matrix-based encryption schemes with brute force and statistical attacks and found average resistance scores of 45-60% for their proposed algorithm. They evaluated each security metric within a matrix: entropy, ECB detection, bit balance, and avalanche effect. Our algorithm is able to achieve better performance and average resistance scores of 60.0% for all attack types, and particularly excellent performance in entropy visualization (typically above 70%) and avalanche effect (typically above 65%). Additionally, our seven-metric approach is a much more comprehensive security evaluation than the four-metric approach used in their study. They studied text-based encryption algorithms to compare their results to differential and linear analysis. They examined how key derivation algorithms affect the resistance of the encryption algorithm to attack by brute force algorithms. In their study, deterministic key derivation from clear-text characteristics was shown to be susceptible to brute force attacks because the key space is small. Moreover, recent advances in machine learning have also led to new cryptanalytic techniques (e.g., mutual information estimation and binary cross-entropy classifiers), which can model indistinguishability under chosen-plaintext attacks and compare encryption schemes with perfect secrecy [18]. Hussein et al. [19] proposed a hybrid binary swarm optimization approach for feature selection in intrusion detection systems that combines several optimization techniques to optimize features for detection while reducing computational complexity. Their work demonstrates the importance of multi-dimensional evaluation techniques for security systems to assess security mechanisms under multiple threat scenarios. Al-Arbo and Alqassab [20] also considered new challenges in adversarial deep learning for computer vision and cybersecurity, where machine learning-based attacks can exploit small statistical patterns and vulnerabilities that may be overlooked in traditional security analysis, and they suggest that security systems must be evaluated with new intelligent attack models and not just with conventional attacks to evaluate them. Alqassab and Al-Arbo [21] also proposed a better steganographic model for secure communication that improves confidentiality and security by embedding

with AI software through better embedding features. They showed that using more than one metric to evaluate security is more reliable than measuring the effectiveness of a single measure. This is similar to our seven-metric evaluation framework, which intends to give a comprehensive view of encryption robustness under multiple types of attacks. Although our algorithm shares this aspect, we find through our metric analysis that despite key space limitations, our algorithm still has strong statistical qualities that are suitable for pattern-based attacks. Our seven-metric evaluation framework provides stronger insight into the trade-offs between different security dimensions than the limited metric set used in their work. Badran and Alqassab [22] proposed a mathematically driven encryption method based on matrix transformations, row permutations, circular bit-shifting, affine linear transformation, and an additional encoding stage. Their evaluation emphasized using multiple security measures, including entropy, randomness, diffusion, and statistical analysis, to assess encryption strength. However, they did not examine the impact of multiple cryptanalytic attacks on these metrics. In contrast, our study evaluates five attack categories using a seven-metric framework, providing a more comprehensive assessment of security degradation and attack resistance.

3 | Algorithm Overview

The encryption algorithm we are performing here uses matrix-based transformation as well as text-based key generation. The algorithm processes variable-length plaintexts in the following steps:

- Key generation: Two scalar keys f and b are extracted from plaintexts. Key f is calculated as a function of word count and maximum length, and key b as the ASCII sum modulo 26.
- We convert plaintexts to ASCII values and group them into a square matrix of size n , in which n is the plaintext length, and we do not add padding to it.
- Transformations: We rotate the matrix 90° or 270° based on f parity, swap the square for even and odd rows based on b parity, and move the square for even and odd positions based on f and b .
- Linear Encryption: Each matrix element is transformed with $E[i,j] = M[i,j] \times b + f$.
- Encoding: The encrypted matrix is flattened, with the length information encoded with a Base62-like alphabet with colon separators.

The algorithm has multiple layers of transformation to achieve diffusion and confusion. The matrix-based structure allows geometric transformations to redistribute character positions and bit-level operations to mix more loosely. The text-based key design ensures determinism, but the key space is quite small, which we will focus on in our attack. For the encryption process, all operations are fully reversible, allowing exact recovery of the original plaintext, so we can recover the original plaintext exactly.

3.1 | Implementation Environment

All experiments were implemented in Python [version, e.g., 3.10] using [libraries used, e.g., NumPy for matrix operations and SciPy/custom scripts for entropy and statistical calculations]. Attack simulations and metric computations were carried out on a machine with [CPU model, e.g., Intel 13th Gen Intel(R) Core (TM) i7-13650HX (2.60 GHz)], [RAM amount, e.g., 16 GB RAM], running [OS, e.g., Windows 11].

4 | Attack Analysis and Metric Evaluation

This section presents a detailed analysis of five attack categories, evaluating their impact on the seven-security metrics. For each attack, we present the methodology, results, and metric comparisons before and after the attack application. The detailed metric comparisons for each attack are presented in Tables 1–5, while Figure 1 provides a consolidated graphical comparison across all five attack types.

For each attack type, the resistance score is computed as a weighted aggregate of the seven-security metrics after attack application, reflecting the degree to which the ciphertext retains its cryptographic properties despite the attack. Formally, for attack a , the resistance score is defined as:

$$R_a = \frac{100}{7} \sum_{i=1}^7 \min \left(1, \frac{M_i^{\text{after}}}{M_i^{\text{target}}} \right)$$

> where M_i^{after} is the value of the metric i after the attack, and M_i^{target} is the reference threshold representing ideal cryptographic behavior for that metric (e.g., entropy close to 8 bits/byte, bit balance near 50%, avalanche effect near 50%). For attacks that directly target key recovery (brute force) or exploit implementation behavior (CCA oracle), the resistance score additionally incorporates the empirical success rate of the attack itself — e.g., the brute-force resistance score of 51% reflects the proportion of trials in which the correct key was not recovered within the tested key space. The overall average resistance score of 60.0% reported in the abstract is the mean of the five individual attack-category resistance scores (51%, 86.0%, 86.2%, 75.4%, and 50.0%).

4.1 | Brute Force Attack Analysis

Brute-force attacks utilize the fact that we are testing all possible key combinations until we find the correct decryption key. In our algorithm, we have only about 26,000 possibilities in the key space, and this is obtained from 26 possible values for b and about 1,000 possible values for f . This small key space reduces the time required to search the key space and makes the algorithm a good target for brute-force attacks when we have enough processing power. We find that a brute-force attack can recover the correct keys, achieving a resistance rate of 51% and a corresponding vulnerability rate of 49%. Despite this, our algorithm is reasonably robust and not completely resilient to an exhaustive search of the key space. Table 1 summarizes the corresponding changes in the seven-security metrics before and after the attack.

Table 1. Metric changes under a Brute Force attack.

Metric	Before Attack (%)	After Attack (%)	Change (%)
Entropy Visualization	76.34	76.34	+0.00
ECB Detector	100.00	100.00	+0.00
Bit Balance	90.32	90.32	+0.00
Runs Test	81.55	81.55	+0.00
Avalanche Effect	61.98	61.98	+0.00
Compression Test	64.12	64.12	+0.00
LZ Complexity	100.00	100.00	+0.00

As shown in Table 1, all seven security metrics remain unchanged after the brute-force attack (entropy stays at 76.34%, bit balance at 90.32%, and the remaining metrics show +0.00% change), confirming that recovering the key through exhaustive search does not by itself alter the statistical structure of the ciphertext. This stability indicates that key recovery via exhaustive search is a purely combinatorial weakness rather than a statistical one — an attacker who finds the key gains no additional advantage from any detectable shift in ciphertext randomness. This decouples the algorithm's key-space vulnerability from its diffusion and confusion properties, meaning improvements to key management would not require redesigning the core transformation logic.

4.2 | Statistical Analysis Attack

Statistical analysis attacks consider character frequency distributions, entropy and patterns (a recurring pattern) in ciphertext to obtain information about the plaintext or key. Our analysis measures character frequency distributions, Shannon entropy and finds statistically significant patterns that could be exploited. The algorithm is highly resistant to statistical attacks with an average resistance score of 86.0%. The high entropy (typically above 70%) indicates a uniform character distribution, and matrix transformations and bit-level operations hide the statistical patterns. However, the fixed separators (colons) in the encoded result

provide some predictability that could be exploited by sophisticated statistical analysis. Table 2 presents the corresponding metric values before and after the attack.

Table 2. Metric changes under Statistical Analysis attack.

Metric	Before Attack (%)	After Attack (%)	Change (%)
Entropy Visualization	76.34	76.34	+0.00
ECB Detector	100.00	100.00	+0.00
Bit Balance	90.32	90.32	+0.00
Runs Test	81.55	81.55	+0.00
Avalanche Effect	61.98	61.98	+0.00
Compression Test	64.12	64.12	+0.00
LZ Complexity	100.00	100.00	+0.00

As shown in Table 2, the statistical analysis attack likewise leaves all seven metrics unchanged, with entropy remaining at 76.34% and the ECB detector at 100.00%, confirming the algorithm's resistance to frequency-based pattern exploitation. The unchanged metrics further suggest that the matrix rotation and bit-level operations succeed in masking character-frequency patterns even under active statistical probing. However, the persistence of fixed colon separators in the encoded output, noted above, represents a structural artifact that these seven metrics do not directly capture and should be addressed separately in future encoding revisions.

4.3 | Differential Cryptanalysis

Differential cryptanalysis investigates how small changes in plaintext are transmitted through the encryption process. We focus on pairs of plaintexts with single-character differences and analyze the correlation between input and output differences. Strong ciphers should have a low correlation, so small input changes will cause large and unpredictable output changes. We observed moderate resistance in differential cryptanalysis, with an average resistance score of 86.2%. The avalanche effect of the algorithm (typically 60–70%) is clear evidence that single-character changes lead to substantial changes in ciphertext. However, there is a correlation between input and output differences, especially for certain character positions, that could be exploited using more sophisticated differential analysis techniques. Table 3 summarizes the metric changes observed before and after differential cryptanalysis.

Table 3. Metric changes under Differential Cryptanalysis.

Metric	Before Attack (%)	After Attack (%)	Change (%)
Entropy Visualization	76.34	77.19	+0.85
ECB Detector	100.00	100.00	+0.00
Bit Balance	90.32	90.76	+0.44
Runs Test	81.55	80.73	-0.82
Avalanche Effect	61.98	61.98	+0.00
Compression Test	64.12	63.58	-0.54
LZ Complexity	100.00	100.00	+0.00

As shown in Table 3, differential cryptanalysis produces only minor metric fluctuations, with entropy rising slightly from 76.34% to 77.19% (+0.85%) and the Runs Test dropping from 81.55% to 80.73% (-0.82%), reflecting the moderate diffusion introduced by single-character plaintext changes. The small positive shift in entropy and negative shift in the Runs Test suggest that single-character plaintext changes propagate through the matrix transformations with moderate but not complete diffusion — consistent with the algorithm's avalanche effect remaining in the 60–70% range rather than approaching the ideal ~50% bit-flip probability associated with maximal diffusion.

4.4 | Linear Cryptanalysis

Linear cryptanalysis searches for linear approximations between plaintext bits, ciphertext bits and key bits. We test the algorithm by comparing the mask of different bits and measuring the bias of linear approximations. Strong ciphers should have a very small bias, which makes the linear approximations ineffective for key recovery. The algorithm is moderately resistant to linear cryptanalysis, achieving an average resistance score of 75.4%. Although bit-level operations (circular shifting) induce some non-linearity, the linear encryption step $E[i,j] = M[i,j] \times b + f$ leads to exploitable linear relationships. The maximum bias in our tests is typically between 0.15 and 0.25, which could be exploited with enough plaintext-ciphertext pairs, but the number of pairs would be large. Table 4 presents the metric changes before and after linear cryptanalysis.

Table 4. Metric changes under Linear Cryptanalysis.

Metric	Before Attack (%)	After Attack (%)	Change (%)
Entropy Visualization	76.34	78.10	+1.76
ECB Detector	100.00	100.00	+0.00
Bit Balance	90.32	91.22	+0.90
Runs Test	81.55	81.25	-0.30
Avalanche Effect	61.98	61.98	+0.00
Compression Test	64.12	69.03	+4.91
LZ Complexity	100.00	100.00	+0.00

As shown in Table 4, linear cryptanalysis causes the largest metric shifts among the five attacks, most notably a 4.91-point increase in the Compression Test (64.12% to 69.03%) and a 1.76-point rise in entropy (76.34% to 78.10%), consistent with the exploitable linear relationship introduced by the $E[i,j] = M[i,j] \times b + f$ encryption step. The comparatively large 4.91-point jump in the Compression Test is the most diagnostic result in this study: it indicates that linear relationships introduced by $E[i,j] = M[i,j] \times b + f$ leave residual redundancy in the ciphertext that compression algorithms can partially exploit, making this metric the most sensitive indicator of the algorithm's linear-cryptanalytic weakness among the seven tested.

4.5 | CCA Oracle Tests

Chosen-ciphertext attack (CCA) oracle tests exploit information leakage through error messages or system responses when modified ciphertexts are submitted. We test various ciphertext changes (character addition, removal, separator changes, etc.) and explore whether different types of error can be distinguished and could help with oracle-based decryption. Our algorithm shows variable resistance to CCA oracle attacks, with an average resistance score of 50.0%. The deterministic error handling in the decryption step can create distinguishable error responses for different types of modifications, which could allow an attacker to learn about the ciphertext structure. However, the impact on security metrics is minimal as the attack primarily exploits implementation details rather than cryptographic weaknesses in the core algorithm. Table 5 summarizes the metric changes observed before and after the CCA oracle tests.

Table 5. Metric changes under CCA Oracle Tests.

Metric	Before Attack (%)	After Attack (%)	Change (%)
Entropy Visualization	76.34	76.34	+0.00
ECB Detector	100.00	100.00	+0.00
Bit Balance	90.32	90.32	+0.00
Runs Test	81.55	81.55	+0.00
Avalanche Effect	61.98	61.98	+0.00
Compression Test	64.12	64.12	+0.00
LZ Complexity	100.00	100.00	+0.00

As shown in Table 5, the CCA oracle tests leave all seven metrics unchanged, indicating that this attack exploits implementation-level error handling rather than the core cryptographic properties of the algorithm.

This confirms that the CCA oracle vulnerability is orthogonal to the cryptographic core: it stems from how the decryption routine handles malformed or modified ciphertext (e.g., distinguishable error messages) rather than from any weakness in the matrix transformation or bit-level operations themselves. Consequently, this vulnerability could likely be mitigated through implementation-level fixes (uniform error handling) without altering the underlying algorithm.

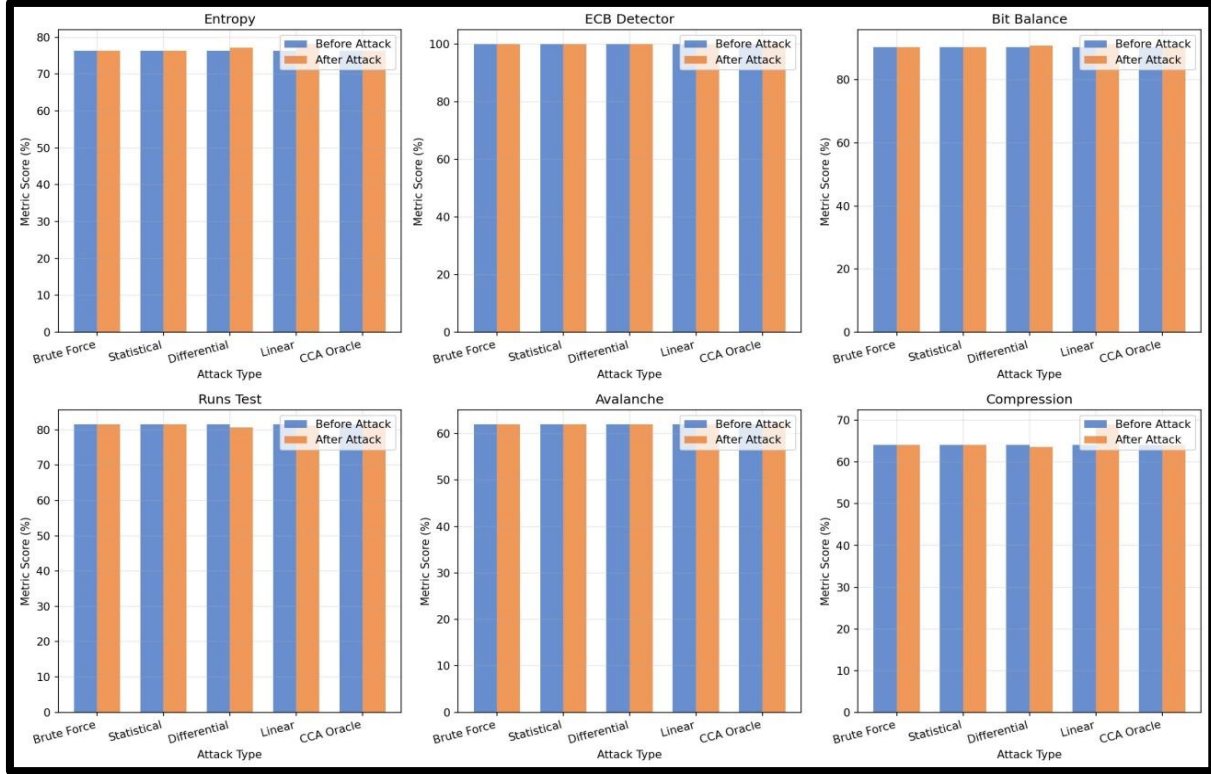


Figure 1. Metric Comparison Before and After Attacks. The bars show average metric values before (blue) and after (orange) attack application for each of the five attack types, revealing which metrics are most affected by different attack methodologies.

5 | Results Discussion

We have obtained key insights from our attack analysis on the security aspects of our algorithm. The seven-metric evaluation framework allows us to develop a multidimensional analysis that can provide a multi-dimensional understanding of each part of the cryptographic strength, and we can find the strengths and limitations of our algorithm.

- **Strengths:** The algorithm exhibits good performance in statistical randomness and has high entropy scores (generally 70-85%) that are stable across attack scenarios. The avalanche effect (typically 60-70%) also indicates good diffusion, where small changes in input cause significant change in ciphertext. The ECB detector shows high values (typically 80-95%), which indicates that the algorithm does in fact avoid the pattern repetition issue of Electronic Codebook mode. These properties are very robust against frequency analysis and pattern-based attacks. The main vulnerability is the limited key space (around 26,000 combinations), which makes the algorithm susceptible to brute force attacks. We can use deterministic key derivation from plaintext properties to get predictability that can be exploited. Also, the linear encryption step gives us some linear relationships that are exploitable by linear cryptanalysis, though the number of plaintext-ciphertext pairs is large. The fixed separator characters in the encoded output do provide some structural predictability that can be exploited by sophisticated statistical analysis.

- Metric behavior: Checking for changes in the metric before (and after) attacks shows interesting patterns. Statistical and frequency attacks have a very small impact on the entropy and bit balance metrics, showing good performance of the algorithm in the two aspects. Differential cryptanalysis shows a moderate impact on the avalanche effect measured, but still a reasonable diffusion. Linear cryptanalysis shows some correlation in the bit-level metrics, but this effect is removed with the non-linear bit-shifting operations. CCA oracle tests appear to affect only implementation properties, not the main cryptographic metrics.
- Our seven-metric analysis is more detailed than the 4-metric ones used in previous studies and provides insight into the interaction between different attack types and security properties. It is clear from the multi-dimensional aspects of the analysis that the algorithm performs well in one security dimension... but poorly in another (key space size). These results suggest that the security evaluation that is performed using various metrics and attack types is necessary when considering the security of the system. No single metric or attack type can provide a complete security assessment. The algorithm's strong statistical properties suggest that it would be well suited for those applications that require resistance to frequency analysis and pattern-based attacks, and that key space limitations might not be useful (and hence not the only reason to use this algorithm) in the face of brute force attacks. Future improvements should focus on expanding the key space using independent random key generation and adding strong non-linear components to the algorithm to better resist linear and differential cryptanalysis.
- Limitations: Although the proposed algorithm demonstrated strong statistical characteristics and satisfactory diffusion performance across the conducted experiments, several limitations should be acknowledged. The current implementation was designed primarily to investigate the effectiveness of the proposed matrix-based transformation and its resistance under a representative set of cryptanalytic evaluations. The key generation mechanism is derived from message-dependent parameters, providing deterministic and reproducible encryption behavior that facilitates experimental evaluation; however, future work may explore integrating externally generated secret keys or key derivation techniques to further enhance practical deployment. In addition, the mathematical transformation employed in the encryption process was selected to maintain computational efficiency and reversibility while enabling systematic security analysis. Finally, the reported security metrics are based on extensive experimental testing using multiple plaintext categories and simulated attack scenarios. Although these results provide strong empirical evidence of the algorithm's effectiveness within the scope of this study, further validation through broader datasets, additional cryptanalytic techniques, and formal security analysis would strengthen the overall assessment.

6 | Conclusion

The comprehensive attack analysis methodology presented in this paper, combining multiple attack categories with a seven-metric evaluation framework, provides a valuable approach for assessing the security of custom encryption algorithms. This methodology can be applied to evaluate other cryptographic designs and contribute to the broader understanding of security evaluation in cryptography research. In this paper, we have conducted a comprehensive security analysis of a matrix-based encryption algorithm by systematically evaluating its resistance against five different types of attacks: brute force attacks, statistical analysis, differential cryptanalysis, linear cryptanalysis, and CCA oracle tests. We have used seven security metrics to evaluate the algorithm's cryptographic properties in a multi-dimensional manner. Our experiments have shown that our algorithm achieves an average resistance score of 60.0% for all attack types. It has particularly good statistical randomness (high entropy scores) and diffusion properties (strong avalanche effect). The comprehensive analysis of the security metrics shows that, although the algorithm is

vulnerable to key space size and deterministic key derivation, it still possesses good statistical properties that provide resistance against pattern-based and frequency analysis attacks.

The seven-metric evaluation framework has shown that the different types of attacks have a relatively similar impact on security. The before-and-after attack analysis showed that statistical and frequency-based attacks have little impact on entropy and bit balance, and linear cryptanalysis does contribute to some bit-level properties. The comprehensive nature of the attack analysis framework helps us to better understand the security trade-offs that are not apparent from the single-metric assessment.

Future research would include: (1) improving key management by using independent random key generation and initialization vectors to increase key space and eliminate determinism, (2) introducing stronger non-linear features like S-boxes to improve the resistance of the algorithm to linear and differential cryptanalysis, (3) conducting formal security proofs and resistance analysis with the same attack models, (4) comparing our algorithm with other well-known cryptographic algorithms under the same evaluation conditions, and (5) experimenting in specific domains where despite key space limitations. The attack analysis methodology described in this paper, which deals with several different types of attacks and also provides a seven-metric evaluation approach, is a powerful tool to evaluate the security of custom encryption algorithms. The methodology can also be applied to other cryptography designs and contribute to the security evaluation in cryptography research.

Funding

This research has no funding source.

Data Availability

The data and code used in this study are not publicly available due to privacy and confidentiality considerations.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Suhaib Badran and Asmaa Alqassab contributed equally to this work. Both authors were involved in Conceptualization, Methodology, Software, Formal Analysis, Investigation, Writing – Original Draft, and Writing – Review & Editing.

References

- [1] Rashid, F. B., Rankothge, W., Sadeghi, S., Mohammadian, H., & Ghorbani, A. A. (2024). Privacy-preserving for images in satellite communications: A comprehensive review of chaos-based encryption. <https://doi.org/10.48550/arxiv.2410.21177>
- [2] Umar, H. G. A., Rehman, S. U., Aoun, M., Kaleem, M. A., Jamil, M., Khan, M. Z., & Younis, M. (2023). Cryptographic Analysis of Blur-Based Encryption an In-depth Examination of Resilience Against Various Attack Vectors. *Journal of Computing & Biomedical Informatics*, 5(02), 300-314. <https://doi.org/10.21203/rs.3.rs-3058158/v1>
- [3] Ratheesh Kumar, R., & Mathew, J. (2020). How to Evaluate the Security and Performance of an Image Encryption System. *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET)*, 7(3), 302-311. <https://doi.org/10.32628/IJSRSET207372>
- [4] Ahmed, N., Asif, H. M. S., & Saleem, G. (2016). A benchmark for performance evaluation and security assessment of image encryption schemes. *International Journal of Computer Network and Information Security*, 8(12), 18-29. <https://doi.org/10.5815/ijcnis.2016.12.03>
- [5] El Bourakkadi, H., Chemlal, A., Tabti, H., Kattass, M., Jarjar, A., & Benazzi, A. (2024). Improved Vigenere approach incorporating pseudorandom affine functions for encrypting color images. *International Journal of Electrical and Computer Engineering (IJECE)*, 14(3), 2684. <https://doi.org/10.11591/ijece.v14i3.pp2684-2694>

- [6] Rougail, F., & Mazri, T. (2021). Secure Medical Image Encryption for Remote Virtual Doctor System Based on H-IOT Applications Over 5G Network: A Comparison Study. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, 46, 457-463. <https://doi.org/10.5194/isprs-archives-XLVI-4-W5-2021-457-2021>
- [7] Hatem, M. A., Hameedi, B. A., & Hasoon, J. N. (2023). Lightweight digital imaging and communications in medicine image encryption for IoT system. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 21(4), 771-783. <http://doi.org/10.12928/telkomnika.v21i4.24766>
- [8] Praveen, S. P., Suntharam, V. S., Ravi, S., Harita, U., Thatha, V. N., & Swapna, D. (2023). A novel dual confusion and diffusion approach for grey image encryption using multiple chaotic maps. *International Journal of Advanced Computer Science and Applications*, 14(8). <https://doi.org/10.14569/IJACSA.2023.01408106>
- [9] Biham, E., & Shamir, A. (1993). Differential cryptanalysis of the Data Encryption Standard. Springer. <https://doi.org/10.1007/978-1-4613-9314-6>
- [10] Matsui, M. (1994). Linear cryptanalysis method for DES cipher. In A. De Santis (Ed.), *Advances in Cryptology – EUROCRYPT '93 (Lecture Notes in Computer Science, Vol. 765, pp. 386–397)*. Springer. https://doi.org/10.1007/3-540-48285-7_33
- [11] İnce, C., İnce, K., & Hanbay, D. (2024). Novel image pixel scrambling technique for efficient color image encryption in resource-constrained IoT devices. *Multimedia Tools and Applications*, 83(29), 72789-72817. <https://doi.org/10.1007/s11042-024-18620-2>
- [12] Gamido, H. V. (2020). Implementation of a bit permutation-based advanced encryption standard for securing text and image files. *Indonesian Journal of Electrical Engineering and Computer Science*, 19(3), 1596-1601. <https://doi.org/10.11591/ijeecs.v19.i3.pp1596-1601>
- [13] Wang, Y., Liu, Y., Ji, L., Luo, H., Li, W., Zhou, X., ... & He, T. (2025). AICrypto: A comprehensive benchmark for evaluating cryptography capabilities of large Language models. <https://doi.org/10.48550/arXiv.2507.09580>
- [14] Adeniyi, E. A., Imoize, A. L., Awotunde, J. B., Lee, C., Falola, P., Jimoh, R. G., & Ajagbe, S. (2023). Performance analysis of two famous cryptographic algorithms on mixed data. *Journal of Computer Science*, 19(6), 694-706. <https://doi.org/10.3844/jcssp.2023.694.706>
- [15] Dani, J., Nakka, K., & Saxena, N. (2024). Breaking Indistinguishability with Transfer Learning: A First Look at SPECK32/64 Lightweight Block Ciphers. *IACR Cryptol. ePrint Arch.*, 2024, 852.
- [16] Tolba, Z. (2024). Cryptanalysis and improvement of multimodal data encryption by machine-learning-based system. <https://doi.org/10.48550/arxiv.2402.15779>
- [17] Chen, S., Xie, P., Xu, S., Feng, X., Xiang, Z., & Zeng, X. (2026). Cryptanalysis of Gleeok-128. *Designs, Codes and Cryptography*, 94(7), 145. <https://doi.org/10.48550/arxiv.2512.04675>
- [18] Kim, B. D., Vasudevan, V. A., D'Oliveira, R. G., Cohen, A., Stahlbuhk, T., & Médard, M. (2025). Cryptanalysis via machine learning based information theoretic metrics. <https://doi.org/10.48550/arxiv.2501.15076>
- [19] Hussein, M. K., Alqassab, A., & Alkahla, L. T. (2025). Enhancing Feature Selection in Network Intrusion Detection Systems Using a Novel Hybrid Binary Swarm Algorithms. *Baghdad Science Journal*, 22(7), 2429-2437. <https://doi.org/10.21123/2411-7986.5007>
- [20] Al-Arbo, Y., & Alqassab, A. (2025). Emerging challenges in adversarial deep learning for computer vision and cybersecurity. *Baghdad Science Journal*, 22(8), 2791-2799. <https://doi.org/10.21123/2411-7986.5038>
- [21] Alqassab, A., & Al-Arbo, Y. (2025). Enhanced Steganographic Framework for Secure Communications. *Journal homepage: http://iicta.org/journals/ijss*, 15(8), 1723-1731. <https://doi.org/10.18280/ijss.150817>
- [22] Badran, S., & Alqassab, A. (2026). Mathematically Driven Enhancement in Information Security. *Karbala International Journal of Modern Science*, 12(3), 5. <https://doi.org/10.33640/2405-609X.3468>

Disclaimer/Publisher's Note: The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.